普通高等教育“十一五”国家级规划教材

“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息安全测评与风险评估

向宏　傅鹂　詹榜华　著
何德全　赵泽良　审

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书分为三部分共 13 章。第 1 部分（第 1、2 章）介绍信息安全测评思想和方法，是全书的灵魂；第 2 部分（第 3 章至第 6 章）介绍测评技术和流程；第 3 部分（第 7 章至第 13 章）介绍风险评估、应急响应、法律法规和信息安全管理体系。全书涉及了信息安全等级保护、风险评估、应急响应和信息安全管理体系等相关的国家标准，均属于我国开展信息安全保障工作中所依据的核心标准集。

本书通过理论与实践紧密联系的方式，向读者介绍如何依据国家有关标准要求进行信息系统的安全测评和风险评估。读者读完本书之后，既可掌握国家有关标准，更能在实际工作中去贯彻执行这些标准。

本书主要是针对全日制普通高等学校信息安全专业高年级本科生编写的，但从事信息安全测评工作的有关读者也可从中获得借鉴。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

信息安全测评与风险评估/向宏，傅鹂，詹榜华著. —北京：电子工业出版社，2009.1
普通高等教育“十一五”国家级规划教材.
“信息化与信息社会”系列丛书之高等学校信息安全专业系列教材

ISBN 978-7-121-07992-4

Ⅰ.信… Ⅱ.①向… ②傅… ③詹… Ⅲ. 信息系统—安全技术—风险分析—高等学校—教材
Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2008）第 199121 号

责任编辑：刘宪兰　　徐蔷薇
印　　刷：北京中科印刷有限公司
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：26.5　字数：606 千字
印　　次：2009 年 1 月第 1 次印刷
印　　数：4 000 册　　定价：36.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

总　　序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会一直在按照党中央、国务院领导同志的要求就信息化前瞻性、全局性和战略性的问题进行调查研究，提出政策建议和咨询意见。在做这些工作的过程中，我们愈发认识到，信息技术和信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力，大量培养符合中国信息化发展需要的人才已成为国家信息化发展的一个紧迫需求,成为我国应对当前严峻经济形势，推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。2006 年 5 月，我国《2006—2010 年国家信息化发展战略》公布，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会一直致力于通过讲座、论坛、出版等各种方式推动信息化知识的宣传、教育和培训工作。2007 年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。编写该系列丛书的目的，是力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

考虑当前国家信息化人才培养的需求、各个专业和不同教育层次（博士生、研究生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，“信息化与信息社会”系列丛书编委会采取了集中全国优秀学者和教师、分期分批出版高质量的信息化教育丛书的

方式，根据当前高校专业课程设置情况，先开发“信息管理与信息系统”、“电子商务”、“信息安全”三个本科专业高等学校系列教材，随后再根据我国信息化和高等学校相关专业发展的情况陆续开发其他专业和类别的图书。

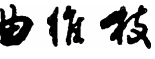
对于新编的三套系列教材（以下简称系列教材），我们寄予了很大希望，也提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时地把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用的目的，等等。

为力争出版一批精品教材，“信息化与信息社会”系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入到各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；第三，要求各专业编委会对教材大纲、内容等进行严格的审核，并对每一本教材配有一至两位审稿专家。

如今，我们很高兴地看到，在教育部和原国务院信息化工作办公室的支持下，通过许多高校教师、专家学者及电子工业出版社的辛勤努力和付出，“信息化与信息社会”系列丛书中的三套系列教材即将陆续和读者见面。

我们衷心期望，系列教材的出版和使用能对我国信息化相应专业领域的教育发展和教学水平的提高有所俾益，对推动我国信息化的人才培养有所贡献。同时，我们也借系列教材开始陆续出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、老师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员以及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，还是一个初步的尝试。其中，固然有许多的经验可以总结，也难免会出现这样那样的缺点和问题。我们衷心地希望使用系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。



2008 年 12 月 15 日

序　　言

人类走过了农业社会、工业社会，如今正处于信息社会的伟大时代，“信息社会”这个词语无疑已经家喻户晓，信息化的大潮正席卷着世界的每一个角落。地球两端，万里之隔，人们能通过互联网与亲朋畅快交流，音容笑貌犹如就在眼前，真正是天涯变咫尺；分支机构遍布全球的庞大企业运转有条不紊，各机构协作顺畅，其功能强大的信息系统功勋卓著；分析复杂神秘的生物基因，预测瞬息万变的天气趋势，有了容量惊人的数据库系统和“聪明绝顶”的高性能计算系统，科学家们如虎添翼。总之，人类处处受益于信息化成果并正在信息化这条大道上加速前进，决不会放慢脚步。

然而，阳光之下总会有阴影，人类越依赖于信息系统，信息安全问题就越发突显。关于信息安全的形形色色的新闻日益频繁地见诸于媒体：某银行数据库数据被窃取导致客户信息泄露，终使客户惶惶不安，银行面临信任危机；某计算机病毒大肆泛滥，无数用户系统瘫痪，让相关企业损失惨重；某国军方网络被黑客侵入，军事机密竟被人如探囊取物般轻易窃取……这样的事件一再提示我们，信息安全问题是社会信息化发展进程中无法回避的客观产物，只有主动积极地面对和解决这一问题才能保障信息化的顺利推进，确保经济、社会的稳定乃至国家的安全。

目前，世界各国政府在信息安全领域的重视程度正在不断加大，并纷纷推出了本国的相关标准、规范或法律，大力扶持高校和其他科研机构对信息安全问题的研究，同时采取各种措施促进信息安全领域的人才培养以满足本国信息化建设的需要，为本国的信息产业发展提供中坚力量。特别是一些信息化进程起步较早，水平较高的发达国家，其信息安全领域的研究水平和产业化程度已相当令人瞩目。

我国正处于信息化建设的关键阶段，2006 年发布的《2006—2010 年国家信息化发展战略》更是从战略的高度指出了推进信息化对我国经济建设和国家发展的重要作用，规划出了新时期我国信息化发展的宏伟蓝图。由此可见，我国的信息化建设和信息产业正面临前所未有的机遇和挑战。

正是在这样的时代背景下，信息安全问题越来越引起全社会上下的广泛关注。信息安全领域必须不断提高研究水平以满足经济建设和国家安全的需要，为我国信息化建设的大踏步前进保驾护航，为创建和谐社会，实现可持续发展贡献力量。因此，大量高素质的信息安全人才成为了最急需、最宝贵的资源。

康有为曾经说过：“欲任天下之事，开中国之新世界，莫亟于教育”。我们的国家要想不断发展科技，增强国力，开创出我们自己富强文明的“新世界”，必须加大力度进行信息化建设。而要使我国的信息化水平走在世界前列，全面提高信息安全领域教育水平，特别是促进高等学校信息安全专业对相关人才的培养和教育，就成为了成败的关键。高等学校信息安全系列教材的编撰就是希望能够为我国的信息安全领域专业人才的培养、为我国信息化水平的腾飞助一臂之力。

信息安全专业教育有其自身的特点，要求学习该专业的学生能够将系统知识与专业知识有机结合，在注重提升理论高度的同时还要能够把理论知识与工程实践紧密联系起来。本系列教材针对高等学校信息安全专业教育的这些特点，同时根据其知识体系、教育层次和课程设置，规划了教材的内容，增加了实际案例，力争做到既紧跟前沿技术的发展，又不失扎实的基本理论和生动活泼的形式，使学生能够学以致用。本系列教材从不同角度论述和总结了信息安全领域的科学问题，有着较强的适用性，既可作为高等学校信息安全专业和相关专业本科生的教材，也可以作为非信息安全专业的公共教科书，同时还可以作为从事信息安全工作的科研技术人员和管理人员的培训教材或参考书，使其了解信息安全相关关键技术和发展态势。

信息安全科学在不断发展，我们也将会努力使本系列教材适应和紧跟这种发展的节奏，使我们培养的信息安全人才能够与时俱进，用自己的所学共筑我国信息安全的万里长城。

限于作者的水平，本系列教材难免存在不足之处，敬请读者批评指正。

高等学校信息安全专业系列教材编委会

2008 年 10 月

前　言

“读万卷书，行万里路”是古人对理论联系实际的最好诠释。面对虚拟空间中纷纷建立起来的形态各异的信息大厦，为了保证它们的建筑质量，世界各国标准化组织均出台了众多的安全标准。这就是本书撰写之前所面临的“万卷书”。如何在信息系统的设计、施工、验收和运行等阶段进行安全检查，就是本书希望做到的在虚拟空间“行万里路”。

作为国内高校信息安全专业本科教材，我们将本书定位为“在国家有关标准的指导下进行信息安全工程作业的参考手册”，并希望以此弥补高校教材在这方面的不足。

在撰写本书的时候，我们首先想到的就是“实用性”。考虑到本书的读者群主要是全日制普通高校信息安全专业的高年级本科生，即将面临社会对他们从事信息安全工作的能力和水平的检验。因此，为了满足我国目前正在开展的信息安全保障工作对测评人员的急迫需求，我们在国家已经颁布实施的众多安全标准中，筛选了“信息安全等级保护”和“信息安全风险评估”这两大类标准作为本书的知识主体，同时也参考了部分已经制定完成但仍处于报批阶段的国家标准，如“应急响应”、“信息安全管理体系”等，以使得本书的知识具有一定的前瞻性。

如果仅仅是介绍国家有关信息安全等级保护、风险评估或应急响应等方面的标准，读者可能会感到比较枯燥或难于理解，而且无从下手进行测评。因此本书大量的篇幅被用来进行案例教学。我们设计了三个具有典型意义的大型模拟案例，逐条指导读者去理解、执行这些标准。这三个模拟案例的设计目的分别是：“天网”（电子政务）系统主要针对信息安全等级保护的测评；“数字兰曦”（企业信息化）主要针对信息安全的风险评估；“南洋烽火”（校园信息系统）主要针对信息安全应急响应计划的制定和演练。

本书的第二个特点是科学性。作为自然科学和社会科学的交叉学科分支，信息安全测评与风险评估有其自身的特殊规律。为了探索这个规律，我们希望读者在进入这个领域之初就应当具备实事求是的科学态度。因此本书的第 1、2 章“信息安全测评思想”和“信息安全测评方法”是本书作者希望与读者交流的最重要的心里话。

本书的第三个特点是规范性。作为一名信息安全测评工程师，在工作中的主要依据就是有关国家标准。因此本书对第 2 部分（第 3 至第 6 章）从事信息安全等级保护测评、第 3 部分从事信息安全风险评估（第 7 至第 10 章）、应急响应（第 11 章）和信息安全管理体系（第 13 章）等工作所遵循的相关标准进行了尽量详细的阐述和解释。

我们向读者特别指出的是，本书所强调的“安全测评是科学与艺术的完美结合”这个观点，并最终体现在“安全测评”、“风险评估”和“应急响应”等技术的融合上，形成“信息安全管理体系”。这也是作者将“信息安全管理体系”相关知识的介绍安排在最后一章的良苦用心。此外，考虑到国家标准对相关法律、法规的密切联系，我们在第 12 章专门介绍了国外有代表性的法律、法规以及我国与本书内容相关的法律、法规情况。

本书的第四个特点是（尽量）做到趣味性。“知之者不如好知者，好知者不如乐知者”。我们希望本书中所采用的“典故”、“争鸣”、“工具”等小模块能够启发读者的创新思维。同时，我们在全书体例上也采用了格言、序幕、要点、正文、尾声、观感的风格，希望给读者营造一种欣赏戏剧或交响乐般的氛围，从而体会信息安全测评工作的艺术性。为了方便读者阅读，本书设计了一些象形符号：

“三星堆面具”图案代表与正文相关的某个典故或背景故事。

“斗士”图案代表一些值得商榷的观点或看法，鼓励讨论。

“榔头”图案代表用于测评/评估工作时的小工具，谨供读者参考。

“逍遥椅”图案代表我们认为值得读者重视的一些观点或工程经验。

“笔记”图案代表重要的概念或定义。

本书包含了大量的实验案例。我们在进行实验设计的时候，已经充分考虑到本书读者的实验条件和动手练习的可能性，因此我们强烈建议阅读本书的读者在可能的情况下“重现”（reproduce）书中案例分析的实验，这是学习测评技术和方法的最好途径。在此基础上，我们在每一章结束后都以“观感”的形式给出一些补充练习，供读者思考。此外，我们也希望读者能够不受本书实验方案设计思路的束缚，举一反三，创新出更好、更贴切的实验方案。我们也真诚地欢迎读者指出本书可能存在的谬误之处（联系地址：xianghong@cqu.edu.cn）。

本书的三位作者分别来自高校和国内知名安全企业。我们希望能够用这种方式来真正体现我国高等教育“产、学、研”的结合。在本书的编写过程中得到了重庆大学有关师生、重庆市信息安全技术中心和北京数字证书有限责任公司员工的大力支持。作者们愿借此机会向他们表示衷心的感谢，没有他们的鼎力支持和批评指正，我们是不可能完成这个艰巨的任务的。

我们要特别感谢重庆大学吴中福教授在本书整体框架确定方面给予的指导并与我们分享他数十年的育才经验。重庆大学胡海波、方蔚涛、蔡斌、桑军、叶春晓、夏晓峰等骨干教师则承担了本书大量的正文撰写和实验指导等工作。

感谢重庆市信息安全技术中心何湘、张亚妮、胡兵、王磊、黄翠等同仁以及重庆大学软件学院 2005、2006、2007 级研究生在从事相关测评实验及本书校稿过程中做的大量工作；感谢北京数字证书有限责任公司安全事业部翟建军等同行提供众多素材并开展休闲式的讨论，作者从中受益匪浅。

感谢对本书原稿进行审核的专家何德全院士和赵泽良副司长，他们提出了诸多建设性的指导意见，拓宽了我们的视野，使我们更加深刻地认识到强调本教材实用性的重要意义。本书在撰写过程中先后多次聆听了高等学校信息安全专业系列教材编委会顾问沈昌祥院士、高等学校信息安全专业系列教材编委会主任冯登国等专家的建议和指导并从中获益匪浅。感谢教材编委会给我们提供了向本领域许多专家如邬贺铨、周宏仁、高世辑、赵小凡、陈国青、徐愈、刘希俭请教的机会。此外，陈晓桦等专家也对本书的初稿提出了诸多有益的建议；重庆市公安局公共网络监察总队白志、重庆市信息安全产品测评中心廖斌、重庆市国家保密局王晓亚等领域专家对本书架构的酝酿及对国家标准的理解等方面也提供了诸多灵感。在此作者也一并表示感谢，并对由于作者能力有限而未能充分体现上述各位专家的建议或批评表示歉意。希望今后有机会能够进一步弥补本书的种种不足之处。

最后作者要感谢电子工业出版社的刘宪兰等老师在本书成稿过程中给予的各种支持、鼓励和花费的大量心血及三位作者的家人在我们挑灯夜战的时候给予我们的理解和支持。

作者

2008 年 9 月

于重庆大学　民主湖畔

目　　录

第 1 章　信息安全测评思想……1

序幕：何危最险？……2

要点：本章结束之后，读者应当了解和掌握……2

1.1　信息安全测评的科学精神……3

1.2　信息安全测评的科学方法……4

1.3　信息安全测评的贯标思想……6

1.4　信息安全标准化组织……7

1.4.1　国际标准化组织……7

1.4.2　国外标准化组织……8

1.4.3　国内标准化组织……9

1.5　本章小结……10

尾声：三位旅行者……10

观感……11

第 2 章　信息安全测评方法……13

序幕：培根的《新工具》……14

要点：本章结束之后，读者应当了解和掌握……14

2.1　为何测评……14

2.1.1　信息系统安全等级保护标准与 TCSEC……15

2.1.2　中国的计算机安全等级保护标准……18

2.1.3　安全域……19

2.2　何时测评……21

2.3　测评什么……22

2.3.1　外网测评特点……23

2.3.2　内网测评特点……24

2.4　谁来测评……25

2.5　如何准备测评……26

2.6　怎样测评……31

2.6.1　测评案例——“天网”工程……32

2.6.2　启动“天网”测评……33

2.7　本章小结……37

目　录

第 1 章　信息安全测评思想 …… 1

序幕：何危最险？ …… 2

要点：本章结束之后，读者应当了解和掌握 …… 2

1.1　信息安全测评的科学精神 …… 3

1.2　信息安全测评的科学方法 …… 4

1.3　信息安全测评的贯标思想 …… 6

1.4　信息安全标准化组织 …… 7

1.4.1　国际标准化组织 …… 7

1.4.2　国外标准化组织 …… 8

1.4.3　国内标准化组织 …… 9

1.5　本章小结 …… 10

尾声：三位旅行者 …… 10

观感 …… 11

第 2 章　信息安全测评方法 …… 13

序幕：培根的《新工具》 …… 14

要点：本章结束之后，读者应当了解和掌握 …… 14

2.1　为何测评 …… 14

2.1.1　信息系统安全等级保护标准与 TCSEC …… 15

2.1.2　中国的计算机安全等级保护标准 …… 18

2.1.3　安全域 …… 19

2.2　何时测评 …… 21

2.3　测评什么 …… 22

2.3.1　外网测评特点 …… 23

2.3.2　内网测评特点 …… 24

2.4　谁来测评 …… 25

2.5　如何准备测评 …… 26

2.6　怎样测评 …… 31

2.6.1　测评案例——“天网”工程 …… 32

2.6.2　启动“天网”测评 …… 33

2.7　本章小结 …… 37

尾声：比《新工具》更新的是什么？ ····· 37
观感 ····· 38
第 3 章　数据安全测评技术 ····· 41
序幕：谜已解，史可鉴 ····· 42
要点：本章结束之后，读者应当了解和掌握 ····· 43
3.1　数据安全测评的诸方面 ····· 43
3.2　数据安全测评的实施 ····· 45
3.2.1　数据安全访谈调研 ····· 45
3.2.2　数据安全现场检查 ····· 50
3.2.3　数据安全测试 ····· 63
3.3　本章小结 ····· 67
尾声：窃之犹在！ ····· 68
观感 ····· 69
第 4 章　主机安全测评技术 ····· 73
序幕：第一代黑客 ····· 74
要点：本章结束之后，读者应当了解和掌握 ····· 74
4.1　主机安全测评的诸方面 ····· 74
4.2　主机安全测评的实施 ····· 77
4.2.1　主机安全访谈调研 ····· 77
4.2.2　主机安全现场检查 ····· 81
4.2.3　主机安全测试 ····· 105
4.3　本章小结 ····· 115
尾声：可信赖的主体 ····· 115
观感 ····· 116
第 5 章　网络安全测评技术 ····· 117
序幕：围棋的智慧 ····· 118
要点：本章结束之后，读者应当了解和掌握 ····· 118
5.1　网络安全测评的诸方面 ····· 119
5.2　网络安全测评的实施 ····· 120
5.2.1　网络安全访谈调研 ····· 120
5.2.2　网络安全现场检查 ····· 126
5.2.3　网络安全测试 ····· 152
5.3　本章小结 ····· 164
尾声：墙、门、界 ····· 165
观感 ····· 165

第 6 章　应用安全测评技术 167
序幕：“机器会思考吗？” 168
要点：本章结束之后，读者应当了解和掌握 168
6.1　应用安全测评的诸方面 168
6.2　应用安全测评的实施 170
6.2.1　应用安全访谈调研 170
6.2.2　应用安全现场检查 174
6.2.3　应用安全测试 192
6.3　本章小结 212
尾声：史上最“万能”的机器 212
观感 213
第 7 章　资产识别 215
序幕：伦敦大火启示录 216
要点：本章结束之后，读者应当了解和掌握 216
7.1　风险概述 216
7.2　资产识别的诸方面 221
7.2.1　资产分类 221
7.2.2　资产赋值 225
7.3　资产识别案例分析 228
7.3.1　模拟案例背景简介 228
7.3.2　资产分类 230
7.3.3　资产赋值 245
7.3.4　资产识别输出报告 254
7.4　本章小结 255
尾声：我们究竟拥有什么？ 255
观感 256
第 8 章　威胁识别 257
序幕：威胁在哪里？ 258
要点：本章结束之后，读者应当了解和掌握 258
8.1　威胁概述 259
8.2　威胁识别的诸方面 260
8.2.1　威胁分类——植树和剪枝 260
8.2.2　威胁赋值——统计 263
8.3　威胁识别案例分析 265
8.3.1　“数字兰曦”威胁识别 265
8.3.2　威胁识别输出报告 277

8.4 本章小结 278
尾声：在鹰隼盘旋的天空下 278
观感 278
第 9 章 脆弱性识别 281
序幕：永恒的阿基里斯之踵 282
要点：本章结束之后，读者应当了解和掌握 282
9.1 脆弱性概述 283
9.2 脆弱性识别的诸方面 284
9.2.1 脆弱性发现 284
9.2.2 脆弱性分类 286
9.2.3 脆弱性验证 286
9.2.4 脆弱性赋值 287
9.3 脆弱性识别案例分析 288
9.3.1 信息环境脆弱性识别 289
9.3.2 公用信息载体脆弱性识别 291
9.3.3 脆弱性仿真验证 295
9.3.4 脆弱性识别输出报告 308
9.4 本章小结 309
尾声：木马歌 309
观感 310
第 10 章 风险分析 311
序幕：烽火的演变 312
要点：本章结束之后，读者应当了解和掌握 312
10.1 风险分析概述 313
10.2 风险计算 313
10.2.1 相乘法原理 315
10.2.2 风险值计算示例 316
10.3 风险定级 316
10.4 风险控制 317
10.5 残余风险 318
10.6 风险评估案例分析 319
10.6.1 信息环境风险计算 320
10.6.2 人员资产风险计算 320
10.6.3 管理制度风险计算 320
10.6.4 机房风险计算 321
10.6.5 信息环境风险统计 321

10.6.6 公用信息载体风险计算 321
10.6.7 专用信息及信息载体的风险计算 322
10.6.8 风险计算报告 323
10.6.9 风险控制示例 324
10.6.10 风险控制计划 328
10.7 本章小结 329
尾声：“勇敢”的反面是什么 329
观感 330
第 11 章 应急响应 331
序幕：虚拟社会的消防队 332
要点：本章结束之后，读者应当了解和掌握 332
11.1 应急响应概述 333
11.2 应急响应计划 334
11.2.1 应急响应计划的准备 334
11.2.2 应急响应计划制定中应注意的问题 337
11.2.3 应急响应计划的制定 338
11.2.4 应急响应计划的培训、演练和更新 351
11.2.5 文档的保存、分发与维护 353
11.3 应急响应计划案例分析 354
11.3.1 南海大学信息安全应急响应计划示例 354
11.3.2 “南洋烽火计划” 355
11.4 本章小结 364
尾声：如何变“惊慌失措”为“从容不迫” 365
观感 365
第 12 章 法律和法规 367
序幕：神话世界中需要秩序吗 368
要点：本章结束之后，读者应当了解和掌握 368
12.1 计算机犯罪概述 368
12.2 信息安全法律和法规简介 370
12.2.1 美国有关法律 370
12.2.2 中国信息安全法律和法规的历史沿革 379
12.3 本章小结 383
尾声：从囚徒困境说起 383
观感 384
第 13 章 信息安全管理体系 385
序幕：武学的最高境界 386

要点：本章结束之后，读者应当了解和掌握 386
13.1 ISMS 概述 386
13.2 ISMS 主要内容 389
13.2.1 计划（Plan） 390
13.2.2 实施（Do） 397
13.2.3 检查（Check） 398
13.2.4 处置（Act） 399
13.3 本章小结 400
尾声：实力源于何处 400
观感 401
参考文献 403

第 1 章
信息安全测评思想





盗“天火”的普罗米修斯

不唯书，不唯上，只为实。

——陈云

序幕：何危最险？

“居安思危，思则有备，有备无患。”（《左传·襄公十一年》）

“福生于微，祸生于忽。”（《说苑·谈丛》汉/刘向）

信息时代有新危，虚拟空间既给人们带来福，也引来祸；从层出不穷的网络安全事件、黑客传奇，到现代高科技战争中的“网络战”、“信息战”，使得信息安全成为了一个令人神往并富有挑战性的热点话题，也给信息安全蒙上了一层神秘的面纱，更让人觉得那虚幻的空间中孕育着真实的危险……

什么最危险？不清楚危险的状况最危险！

如果不清楚信息系统的安全状况，就会“祸生于忽”，而一旦了解了它的安全状况，就有了思想准备，从而决定是否采取相应的预防措施，就能“有备无患”。然而，由于信息本身不可捉摸的特点，信息系统的安全状态不像现实生活中其他系统那样直观、一目了然，更需要科学、规范、专业的判断。

从本章开始，我们将陆续向读者全面、系统地介绍信息安全测评的思想、方法、理论和技术。我们将看到，在令人眼花缭乱的信息安全新闻报道的背后，信息安全测评实际上蕴涵着丰富的思想内涵、严肃的科学精神、严谨的工作作风、严格的测评流程以及极具魅力的测评技巧，是一个科学与艺术圆满结合的领域。在信息系统的安全测评工作中，一名合格的安全测评工程师不仅要有丰富的想象力和创造力，在工作中还要一丝不苟地遵循国家的有关标准规范。

要点：本章结束之后，读者应当了解和掌握

- 什么是信息安全测评的科学精神？
- 什么是信息安全测评的科学方法？
- 什么是信息安全测评的贯标思想？
- 国内外信息安全标准化组织有哪些？

1.1　信息安全测评的科学精神

如果有读者认为信息安全测评就是从事神秘的“hacker”工作，对此我们不敢苟同。我们认为信息安全测评首先是探索真理、发现真相的科学。因此，与其他自然科学一样，信息安全测评也遵循着一般的客观规律。要掌握好信息安全测评的理论、方法和技术，首先应该明确一名安全测评工程师应该具备什么样的科学精神和素养？这是从事信息安全测评工作的前提和基础。有了这些科学精神，再加上训练有素的工作作风和您偏爱的某种 hacker 气质，也许就是作者心目中的安全测评工程师了。

那么，首先要具备什么样的科学精神呢？我们认为，“怀疑、批判、创新、求实、协作”是一名科学工作者必须具备的科学素养，同样也是指导我们进行信息系统安全测评的基本精神和思想。

这种科学精神源自于五百多年前的文艺复兴及其后来的启蒙运动（Enlightenment）。从 16 世纪开始，欧洲一批批进步的宗教人士、哲学家、科学家和艺术家们前赴后继，对万能上帝存在的合理性提出质疑，对中世纪欧洲宗教法庭的权威发起挑战，终于“将科学从神学婢女的地位中解放出来。”1919 年发生在中国著名的“五四”运动，请来的“德先生、赛先生”（民主、科学），则是这场伟大的启蒙运动在古老东方的美妙回声，并持续影响着一代代中国人。尽管这场人类历史上轰轰烈烈的思想解放运动不属于本书撰写的范畴，但请读者记住，包括信息安全学科在内的各门自然科学的发展深受其影响。而作为一门新兴的 IT 学科分支，信息安全测评也必将从前辈们的思想源泉中源源不断地吸取营养。



1964 年 6 月，中国自主研发的第一代战略导弹“东风 2 号”在发射架上整装待发。科学家们却在为一个关键问题苦苦思索：为了提高导弹的射程，必须增加火箭燃料，然而燃料箱却早已加满。这时一位年轻的中尉提出一个不可思议的建议：减少部分燃料反而可以增加射程！人微言轻的中尉提出的建议并没有引起专家们的重视，于是他鼓足勇气走进了钱学森的办公室。钱老为这位年轻人大胆的思路和精确的计算所折服，当即拍板，从燃料箱中卸载数百公斤燃料！随后“东风 2 号”腾空而起，准确命中目标，达到了设计要求。这位年轻人就是后来中国著名的火箭总设计师王永志。

如果读者觉得上面这些“说教”非常抽象，那么就换个角度来思考吧。设想您作为一名信息安全测评工程师，正在对一个信息系统，如某重要金融信息系统进行安全测评。该信息系统建设之前，已经通过了众多专家的评审。现在您发现这个投入了巨资的建设方案并不合理。请问您的质疑有依据吗？您的质疑合理吗？你能实事求是地指出问题出在什么地方吗？您的领导和其他测评工程师支持您吗？

1.2　信息安全测评的科学方法

如果说信息安全测评工作最主要的方法是**系统科学/系统工程**的方法，有的读者可能会感到生疏或迷茫。那么让我们换一个角度来思考吧。

您知道 Windows 操作系统，如 Windows 2003 有多少行代码吗？5000 万行！参与开发与测试的人员接近 8000 人。而这仅仅是一个大型信息系统的某一台 PC 终端可能安装的若干软件之一。

您知道现代超大规模集成电路（VLSI）是一个什么概念吗？Intel 公司利用纳米工艺制造的 45nm Penryn Wolfdale 双核芯片，集成了近 4 亿个晶体管，核心面积仅为 107mm^2（一个手指甲大小）！而这仅仅是一台计算机中若干硬件的一部分。

您知道一名配备得有单兵数字化作战系统的士兵在作战时，身后有多少软、硬件在支撑他吗？太空中有数百颗卫星、天空中有成千架作战飞机、地面上有成群的战车火炮、大海中有各种军舰。而这些“武装到牙齿”的战争怪兽的指挥中枢，又是由千千万万的计算机软、硬件构成的。他们相互交织在一起，构成了一个庞大的“人–机合一”的信息网络……

我们在这里无意扮演桑鲁卓公主的角色来讲述信息时代“一千零一夜”的故事，但想象力丰富的读者应该对现代信息系统的**复杂性**有了一个大概的认识了吧？



中国学者何德全等人提出，要从开放复杂巨系统和“综合集成研究厅体系”的角度来思考和研究信息安全问题。然而这一理论也与其他复杂性理论一样，存在某些不足。中国人民大学苗东升指出，目前开放复杂巨系统理论存在一个不可忽视的问题，即如何构建“涌现性”理论，从而提供复杂系统定量研究的理论框架。

现在让我们回到本节的主题，什么是信息安全测评的科学方法？由于我们面临的测评对象往往是一个复杂、庞大的信息系统，“杀牛就得用牛刀”，因此我们需要采用解决系统复杂性的科学方法——系统科学方法。由于篇幅所限，这里仅仅简要介绍系统科学发展的主要脉络，有兴趣的读者可以参见诸如《系统科学》（许国志主编，上海科技教育出版社.2000）等著作。熟悉这部分内容的读者则可以进入下一节。

纵观人类科学发展史，我们可以看到人类对包罗万象的自然规律的认识经历了一个螺旋循环又不断向上发展的过程，古希腊人最早发明了“系统”这个词，表示“部分之和形成整体”的意思。中国古代大哲人老子的“道生一、一生二、二生三、三生万物”也具有浓厚的系统思想，从某种程度上可以这样讲，中国人最主要、最自然的哲学观点就是系统论观点。这种人类早期认识客观世界的思想方法称为“原始系统论”。而世界上最早将系统科学的思想运用在工程技术中的著名案例当属两千多年前中国的“都江堰”水利工程：“鱼嘴分水堤”自动分流，“飞沙堰溢洪道”自动排沙，“宝瓶口引水口”自动调节流量……“都江堰”整体工程设计之宏伟、各个子系统环环相扣之巧妙，

无一不体现了系统科学的精髓。我们甚至可以这样评价：“没有当年的都江堰，就没有今日的天府之国”。都江堰水利工程在经历了“5.12”汶川 8 级毁灭性大地震后，损失轻微，更让人值得深思。有趣的是，李冰父子的治水思想与我们今天“治信息”的思想有着异曲同工之妙……

随着欧洲文艺复兴运动的兴起，人类认识客观世界的方法从原始的系统论观点向“还原论”转化，其特点是使用分析、分解的方法和演绎、精确的数学工具，对分解后的最小部件进行定量的刻画，然后又回过头来逐级叠加，形成对系统整体的定量描述。这种分析论或者还原论的方法极大地促进了人们对客观世界的认识，并形成了我们今天所掌握的各门自然科学理论，如物理、化学、生物等科学。但另一方面，还原论的科学方法在取得巨大成功的同时，也带来了学科分割、“只见树木不见森林”等弊端。

进入 20 世纪之后，随着人类对宏观、微观世界认识的不断深入，美国的“曼哈顿工程”计划、“阿波罗工程”计划、前苏联的“东方”计划、中国的“561 工程”计划、“921 工程”计划、“嫦娥工程”计划等，由于所涉及的学科非常广泛，管理非常复杂，所以系统科学及系统工程的思想得以进一步发展。人们在吸收了还原论的优点之后，形成了定性分析和定量计算相结合的现代系统科学思想，并开创了以欧洲的“复杂巨系统理论”、美国圣菲研究所（Santa Fe Institute）“复杂性理论”和中国的“开放的复杂巨系统理论”等为代表的现代系统科学理论框架。图 1.1 是关于人类科学发展观与系统科学关系的“龙卷风”模型示意图。

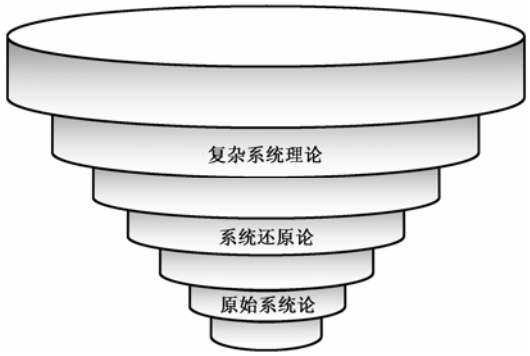


图 1.1　“龙卷风”模型示意图

而在目前方兴未艾的信息科学、信息安全学科以及信息安全测评学科分支中，系统科学的理论也正在发挥着主导作用。信息安全测评工作的最大特征就是要求测评工程师具有“系统科学”的视野和方法。这里的“系统科学”具有三层含义：一是从事测评的不是一个人，而是一个团队，也就是 1.1 节中谈到的“协作”。对测评团队的组织和管理要有系统科学的方法，从而保证测评质量。二是测评的对象往往不是一个单一的软件或硬件，而是一个复杂、庞大并且不断变化的信息系统，本身具有“自组织、自演化”的系统科学特征；三是测评过程中要贯彻“人–机合一”的系统科学思想，这也是本书出

现频率最高的词汇之一。随着本书各章内容和案例的展开，读者对此将会有更深刻的认识。

1.3　信息安全测评的贯标思想

如果说信息安全测评与其他自然科学，如爱因斯坦的相对论、孟德尔的遗传学、香农的信息论等这些“自由发挥”的科学探索和研究相比较有什么最大区别的话，那就是测评工作首先有一个限定的框架，所有的测评活动都是在这个框架之内进行的。这个框架就是国际化标准组织（ISO，International Organization For Standardization）和世界各国根据自身特点颁布实施的各种标准规范。测评工作就是对标准规范的贯彻执行，用我们这行的“行话”来讲，即为“贯标”。



贯标（execution of standards），指测评人员在测评活动中严格遵循相关标准的行为。

信息安全测评是信息安全工程学科的一个分支。而对于一门工程学科而言，其工程技术标准规范的制定与颁布实施，标志着这门学科已经走向成熟。信息安全测评工作与其他工程测评工作一样，扮演的是“质量检查员、监督员、审核员”的角色，或者通俗地讲，是从事“鸡蛋里面挑骨头”的、吃力不讨好的工作。然而为了保障信息系统安全运行，这个角色又是必不可少的。还记得前面举的那个例子吗？如果一个投资巨大的信息系统在安全建设方面有问题，您凭什么来质疑它呢？为了体现测评结果的客观性、科学性和公正性，所有测评工作都必须严格遵守国家有关标准规范并遵循严格的测评流程，即“贯标”流程，这是一名测评工程师“求实”科学精神的具体体现。信息安全测评标准是一个非常庞大的体系，这将在第 2 章“信息安全测评方法”中予以介绍。在这里要告诉读者的是，测评工程师贯标的主要依据是中国有关信息系统安全评估的系列标准，如《信息系统安全等级保护基本要求》、《信息安全风险评估指南》，等等。

但愿“严肃的科学精神”、“严谨的工作作风”和“严格的贯标过程”“三”严要求等内容没有吓跑那些希望培养自己“hacker”技能的读者。这里还需要特别指出的是，贯彻国家有关信息安全测评标准的过程，是体现一名测评工程师“工程规范与艺术创造”完美结合的过程，也是信息安全测评工作最富有魅力的地方之一。从工程规范的角度来讲，国家标准指明了一个信息系统所要达到的各项安全指标，这是测评工作的基线（baseline）和基准（benchmark），是最基本的要求。从艺术创造的角度来讲，由于信息系统的结构各异，所承担的业务工作千差万别，所以世界各国在制定相关标准的时候不会也不可能制定具体的测评方法、方案和步骤。而恰恰在这一点上，就是一名测评工程师“天高任鸟飞、海阔凭鱼跃”，充分发挥其创造力的地方。所以，国外经常把测评工作称之为“测评艺术”（The art of testing），因为它体现了测评工程师（团队）按照有关标准的要求，精心设计各种测评案例来论证一个信息系统是否达到相应安全标准的

创造性过程。我们也将在后面各章中“抛砖引玉”介绍各种测评案例和技术。

信息安全测评的“三严”要求之间构成了一个层次结构分明的体系。底层“严肃的科学精神”是指普适性的科学思想，这是任何科技工作者都应具备的；中间层“严谨的工作作风”是指系统科学方法，这是从事信息科学（当然不仅仅是这个学科）研究的人们应当具备的；顶层“严格的测评流程”是指“贯标流程”，这是从事信息安全测评工作所要遵循的。图 1.2 所示的“蘑菇”模型总结了信息安全测评的科学思想、科学方法、工程标准以及测评对象－复杂信息系统之间的相互关系。

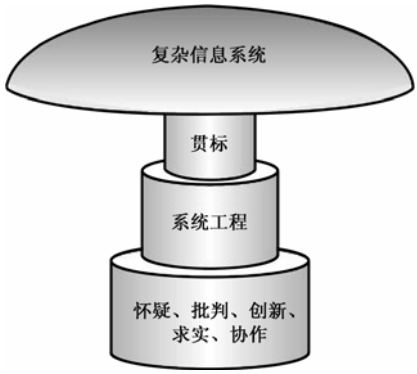


图 1.2　“蘑菇”模型示意图

1.4　信息安全标准化组织

顾名思义，标准化组织就是制定标准规范的权威机构。与其他工程标准规范类似，信息安全标准化组织分为国际和国家两个层面。读者对这些标准化组织情况的略加了解，对今后的测评工作将有所裨益。

1.4.1　国际标准化组织

国际上信息安全标准化工作起源于 20 世纪 70 年代中期，与 Internet 的产生大致同步，80 年代有了较快的发展，90 年代引起了世界各国的普遍关注。目前世界上约有近 300 个国际和区域性组织在从事标准或技术规则制定工作，与信息安全相关的主要标准化组织有 4 个。下面分别做一个简要介绍。

提起大名鼎鼎的国际标准化组织 ISO，读者想必不会陌生，如目前流行的 ISO 9000 质量认证标准等就是 ISO 颁布的众多标准之一。该组织成立于 1947 年 2 月 23 日，是世界最大的非政府性国际标准化组织。ISO 的主要工作是制定国际标准，协调世界范围内的标准化工作，组织各成员国和技术委员会进行信息交流，以及与其他国际性组织进行合作，共同研究标准化问题。ISO 在信息安全标准制定方面扮演了主要的角色。由 ISO 制定的与本书密切相关的信息安全标准包括 ISO 17799（后来的衍生标准 ISO 27001－2005，参见本书最后一章）等。1993 年 6 月，美国、加拿大及英、法 4 国共同起草了信息技术安全评估公共标准 CCITSE（Common Criteria of Information Technical Security Evaluation），简称 CC，该标准是国际标准化组织为了统一现有多种准则的结果。1998 年，经 ISO 9000 认可之后成为国际标准（ISO/IEC 15408，中国对应的国家标准是 GB 18336）。读者可以在 www.iso.org 网站上查询该组织的性质以及制定的相关标准名称等资料。

国际电工委员会（IEC）正式成立于 1906 年 10 月，是世界上成立最早的专业国际标准化机构。在信息安全标准化方面，IEC 成立了涉及电信、电子系统、信息技术和电磁兼容等方面的技术委员会，并制定相关国际标准，如信息技术设备安全（IEC 60950）等。IEC 与 ISO 密切合作，联合成立了 JTC1 分委员会。ISO/IEC JTC1 负责制定的标准主要涉及开放系统互连、密钥管理、数字签名、安全评估等方面的内容。读者可以在 www.iec.org 网站上查询相关内容。

国际电信联盟（ITU）成立于 1865 年 5 月 17 日，所属的 SG17 组主要负责研究通信系统安全标准。SG17 组主要研究的标准内容包括：通信安全项目、安全架构和框架、计算安全、安全管理、用于安全的生物测定、安全通信服务，等等。此外 SG16 组和下一代网络核心组也在通信安全、H323 网络安全、下一代网络安全等标准方面进行了研究。目前 ITU-T 建议书中大约有 40 余份报告都是与通信安全有关的标准。读者可以在 www.itu.int 网站上查询相关资料。

Internet 工程任务组（IETF）始创于 1986 年，其主要任务是负责互联网相关技术规范的研发和制定。目前，IETF 已成为全球互联网界最具权威的大型技术研究组织。IETF 标准制定的具体工作由各个工作组承担，工作组按任务分成八个领域，分别是 Internet 路由、传输、应用领域等，像著名的 IKE 和 IPsec 都在 RFC（Request for Comments）系列之中，此外还有电子邮件、网络认证和密码标准，也包括 TLS 标准和其他的网络安全协议标准等。读者可以在 www.ietf.org 网站上查询相关资料。

1.4.2　国外标准化组织

常言道：“要将命运掌握在自己手中”，安全也是如此。目前，国外信息化发达国家制定本国信息安全标准的代表性机构包括美国、英国、德国、加拿大等国家的标准化组织。由于篇幅所限，我们这里只介绍与本书所参照的标准有密切关系的美英两国的标准化组织。



据报道，生活在“石器时代”的恐怖大亨本·拉登极少使用现代通信工具。然而他在 2001 年导演的“9.11”事件却对信息安全产生了深远的影响。半年之后的 2002 年 3 月，美国政府通过了《联邦政府信息安全管理法案》（FISMA），要求联邦政府各机构以及涉及国家安全的各个重要基础设施管理部门每年必须向美国国会提交本年度信息安全风险评估报告（参见本书“法律、法规”等章节）。随着 FISMA 的通过和 NIST 编制的一系列标准指南的修改和发布，标志着美国联邦政府已逐渐建立和完善了一整套以风险评估为基础、对信息和信息系统进行分级保护的信息安全风险管理框架。

美国国家标准和技术委员会（NIST）成立于 1901 年，是美国联邦政府授权的标准制定机构。该组织在信息安全方面负责为美国政府和商业机构提供信息安全管理相关的标准规范。目前，NIST SP 800 系列成为了指导美国信息安全管理建设的主要标准和参考资料，成为美国和国际信息安全界得到广泛认可的行业标准和

权威指南。

近年来，NIST SP 800 系列最主要的发展是配合 2002 年美国国会通过的 FISMA 法案，建立以 NIST SP 800—53 等标准为核心的一系列认证和认可的标准指南。该标准提供了安全控制的层次化、结构化的控制措施要求，主要包括安全意识和培训，认证、认可和安全评估，配置管理，持续性规划，安全事件响应，维护，介质保护，物理和环境保护，规划，人员安全，风险评估，系统和服务采购，系统和信息完整性 13 个安全管理和运营控制族以及 106 个具体控制措施。读者可以从 www.nist.gov 网站上查询相关资料。本书在后半部分的“风险评估”等有关章节中会对此进行简要介绍。

同样成立于 1901 年的英国标准化协会（BSI，British Standard Institute）是这个老牌工业化国家最主要的标准制定组织。该组织对信息安全的主要贡献是制定了 BS 7799 等标准（后来被 ISO 采用并形成了 ISO 17799 国际标准）。BS 7799 标准是国际上具有代表性的信息安全管理体系标准，如 BS 7799—1：1999（信息安全管理实施细则）标准是组织建立并实施信息安全管理体系的一个指导性的准则，BS 7799—2：2002 标准以 BS 7799—1：1999 标准为指南，按照 PDCA 模型（Plan，Do，Check，Action；俗称“戴明环”），建立、实施及文件化信息安全管理体系（ISMS）的要求。读者可以从 www.bsigroup.com 网站上查询相关资料。本书最后一章将重点介绍信息安全管理体系（ISMS）。

1.4.3　国内标准化组织

信息安全标准是中国信息安全保障体系的重要组成部分，是政府进行信息安全宏观管理的重要依据。虽然国际上有很多标准化组织在信息安全方面制定了许多的标准，但是信息安全标准事关国家安全利益，任何国家都不会轻易相信和过分依赖别国的标准，而是通过自己国家的组织和专家制定出适合本国国情的标准来保护本民族的利益。

目前，中国的标准化组织是按照国务院授权，在国家质量监督检验检疫总局（www.aqsiq.gov.cn）管理下，由国家标准化管理委员会统一管理全国标准化工作，下设有 255 个专业技术委员会。中国标准化工作实行统一管理与分工负责相结合的管理体制，有 80 余个国务院有关行政主管部门和国务院授权的有关行业协会分工管理本部门、本行业的标准化工作，有 31 个省、自治区、直辖市政府有关行政主管部门分工管理本行政区域内本部门、本行业的标准化工作。

成立于 2001 年的**全国信息安全标准化技术委员会**（CITS）负责全国信息安全技术领域以及与 ISO/IEC JTC1 相对应的标准化工作。它是一个具有广泛代表性、权威性和军民结合的信息安全标准化组织。该组织的工作范围是负责信息和通信安全的通用框架、方法、技术和机制的标准化，归口管理国内、外对应的标准化工作。其技术安全标准范围包括：开放式安全体系结构、各种安全信息交换的语义规则、有关的应用程序接口和协议引用安全功能的接口，以及本书所依据的各种安全测评标准，等等。读者可

以从 www.tc260.org.cn 网站上查询相关资料。

中国信息安全标准化工作虽然起步较晚，但是近年来发展较快，特别是加入 WTO 后，中国的标准化工作在公开性、透明度等方面取得了实质性进展。中国从 20 世纪 80 年代开始，本着积极采用国际标准的原则，转化了一批国际信息安全基础技术标准，制定了一批符合中国国情的信息安全标准，同时一些重点行业还颁布了一批信息安全的行业标准，为中国信息安全技术的发展做出了很大的贡献。据统计，中国从 1985 年发布了第一个有关信息安全方面的标准以来到 2007 年年底，共计制定、报批和发布有关信息安全技术、产品、测评和管理的国家和行业标准百余个，为信息安全的开展奠定了基础。与本书密切相关的国家标准主要包括《信息系统安全等级保护基本要求》和《信息安全风险评估指南》等。

1.5　本章小结

- 信息安全测评的“三严”要求
- 信息安全的贯标定义
- 信息安全测评的“蘑菇”模型
- 国际标准化组织与信息安全标准
- 国外信息化发达国家标准化组织与信息安全标准
- 国内标准化组织与信息安全标准

尾声：三位旅行者

当我们知道可能有危险就会预先有所防备，但是这还不够。有这样一则寓言：

三位旅行者夜晚来到一座名山，在客栈里住下，翌日清晨三人先后外出。第一个出门的旅行者什么都没带。第二个旅行者听说路不好走，带了一根拐杖。最后一个出门的旅行者看见天色已变，恐要下雨，就带了一把伞。中午时分，开始下起雨来，道路随后变得泥泞不堪。黄昏时分，三个旅行者都回到了客栈。带了拐杖的旅行者浑身是泥，看来跌得够惨；带了雨伞的旅行者已经是落汤鸡。

奇怪的是，什么都没带的旅行者却好端端的，另外两个旅行者感到纳闷，问他道：“你什么都没带，怎么会好端端的呢？”空手旅行者看了看两人，没有立即回答，先问带了拐杖的旅行者：“你没带雨伞却没有被淋湿，带了拐杖却反倒摔得浑身是泥，怎么回事？”拐杖旅行者答道：“下雨时，我因为没带伞，所以很小心地躲着雨，走走停停，就没有被淋湿。雨间隙中，我用拐杖拄着在泥泞路上走得很快，跌倒了几次。”空手旅行者又问雨伞旅行者：“你没有带拐杖却为什么没有摔得满身是泥，带了雨伞却倒是湿得像个落汤鸡呢？”雨伞旅行者说：“我没有拐杖，所以走得很小心，择好路而行，就没有跌倒。大雨时，我仗着有雨伞，思忖用不着躲避，最后还是被淋湿了。”

“这就对了”，空手旅行者笑着说，“你们的情形就是我的答案了：我没有拐杖也没有雨伞，雨来了我就要躲避，路泥泞我就要小心，所以既没有摔成泥人儿也没有被淋成落汤鸡。”

有了先进的“装备”是不够的，还要有理念和意识，没有居安思危的理念和意识，优势反倒是劣势，这就是辩证法。

观感

（1）与国外系统科学的理论相比，中国现代系统科学理论的特点是什么？代表人物有哪些？

（2）美国圣菲研究所（Santa Fe Institute）是一个什么机构？请在网上查阅该机构的相关介绍。

（3）请在网上查阅中国从事信息安全测评的机构名称。

（4）按照国家有关规定，一个重要信息系统的安全要求定为“三级”，这是什么意思？请在相关网站资源上查找三级系统的定义，并阐述国家哪些标准定义了信息系统安全等级。

（5）请在网上查阅德国、法国和加拿大等国制定信息安全标准的有关机构名称和相关标准。

（6）www.infosec.org.cn 是一个什么网站？中国关于信息安全的主要网站有哪些？请在网上进行相关资料的收集并给出您对这些资源网站的评价。

（7）www.cert.org 是一个什么机构？请在网上查阅该机构的相关介绍，浏览该网站信息之后给出您对它的评价。

（8）FIRST 是一个什么机构？请在网上查阅该机构的相关资料。

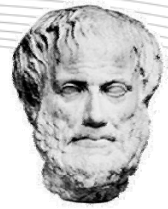
（9）SANS 是一个什么机构？请在网上查阅该机构的相关资料。

（10）在从事信息系统安全测评工作中，一个信息系统当初的建设方案是否也应该纳入测评过程之中？无论是与否，都请阐述你的理由。

（11）现代系统科学理论中，无论是国外的“涌现理论”还是国内的“综合集成研究厅体系”，在对复杂系统进行定性定量综合分析时均各有优、缺点，因此中外专家学者急需通过实际案例来论证其理论的正确性。不少学者把目光投向了互联网这个正在不断“自组织、自生长、自演化”的复杂信息系统。有人甚至绘制了全球互联网的图形。请使用 Google 去检索“internet map”，看看有什么新颖的发现。对于如此复杂的信息系统，您认为保障信息安全的切入点是什么？

第 2 章
信息安全测评方法





亚里士多德雕塑

遂古之初，谁传道之？

——屈原《天问》

序幕：培根的《新工具》

1620 年，大英帝国位高权重，但对国务活动却心不在焉的培根爵士（Francis Bacon）出版了一本学术专著《新工具》，向古希腊科学巨匠亚里士多德（Aristotle）的代表作《工具》发起了挑战，为波澜壮阔的启蒙运动摇旗呐喊，并且奠定了现代实验科学的基础。

在本章里，我们将怀抱滑板冲向科学前辈们浩瀚的思想海洋，向读者介绍信息安全测评这门典型的实验科学的研究方法。当然，我们不会匍匐在前辈们的脚下，照本宣科地介绍实验科学方法论，因为这样做即使能获得培根先生的宽恕，恐怕也仅仅是在信息安全测评行业多了一群现代东施。

通俗地讲，信息安全测评就是回答 5W+H 的问题，即 Why、When、Which、Who、What 和 How。读者将看到，对上述问题的回答将形成一个系统性、规范性的整体“安全解决方案”。

要点：本章结束之后，读者应当了解和掌握

- 为什么要进行信息安全测评（why）？
- 什么时候进行信息安全测评（when）？
- 哪些信息系统需要安全测评（which）？
- 有哪些测评队伍（who）？
- 信息安全测评要做什么准备工作（what）？
- 怎样进行信息安全测评（how）？

2.1 为何测评

“为何测评”这个问题貌似简单，实则不然。如果读者的答案仅仅是“因为重要，所以必须”这一类的八股语言，您可能要面对委托您进行测评的客户愤怒和鄙视的表情。

对信息系统进行安全测评是对信息系统的建设质量进行评判的**必要环节**。无论是政



最早将“可信”的概念引入到当代计算机安全领域中来的应当是美国国防部颁布的 TCSEC 标准。然而要将“可信”这个人文科学、社会科学的概念与一板一眼的计算机联系起来，却是一个新颖而巨大的挑战，也是现在炙手可热的研究课题（可信计算，TC，Trusted Computing,)。“人非我族，其心必异”。这句古老、严酷而又无可奈何的“真理”在虚拟空间中依然适用。A 国绝对可信的系统对于 B 国而言却是处处不可信。“自由软件运动”的创始人之一 Richard Stallman 等人甚至嘲讽“可信的计算”是“背叛的计算”（TC，Treacherous Computing)。

府、社会还是企业花费巨资建设的电子政务、电子商务、企业信息化等平台，都如同虚拟世界中的一幢幢“信息高楼”。这些信息高楼是否按照国家有关标准进行设计、施工、验收和运行维护？其工程质量是否达到“抗震”设计要求？是否有“烂尾楼”或“危房”？是否有垮塌的风险以及这个风险有多高等问题将直接影响到这些复杂系统的应用范围和使用寿命。为此，各国政府均出台了（见本书第 1 章）一系列相关标准规范，以确保这些信息系统具备统一的安全质量，这些安全质量标准是整个信息系统建设质量体系的有机组成部分。而信息安全测评工程师的首要职责，就是在测评工作中**贯彻**这类安全标准。因此，为什么要进行信息安全测评，就是因为要贯彻国家标准规范，保证在规划、设计、建设、运行维护和退役等不同阶段的信息系统满足统一、可靠的安全质量要求。正如本书第 1 章所介绍的那样，国内外进行信息安全标准制定的组织非常多，颁布实施的标准体系也非常庞大，因此，下面我们集中精力介绍与本书信息安全测评密切相关的标准规范体系框架。

2.1.1　信息系统安全等级保护标准与TCSEC

“信息系统安全等级保护标准与 TCSEC”标题可能让初次接触这个领域的读者感到比较困惑。让我们转换一下思考的角度。假设您是日本东京一个著名建筑事务所的建筑设计师。您在设计东京银座商业区摩天大楼的时候，需要考虑什么安全因素呢？当然您需要考虑到日本是一个地震多发区域，而东京银座又是一个极为重要的金融区。因此在设计中需要考虑高层建筑对不同地震等级的抗震强度，同时还需要考虑到一旦发生地震可能带来的次生灾害影响（山体滑坡、泥石流、堰塞湖等对建筑物的影响，建筑物垮塌对金融、商业的影响等）；同样的，如果您是中国长江三峡大坝的设计师，您需要根据长江水域“10 年不遇、20 年不遇、50 年不遇、100 年不遇”的抗洪要求来设计三峡大坝，同时也需要考虑一旦溃坝给长江中下游地区带来的影响（洪水次生灾害风险分析）。**根据一个信息系统受到破坏后可能带来的严重后果，来对该信息系统进行分级保护**的思想其实也是一样的道理。



系统定级（system classification）。根据一个信息系统受到破坏后可能给个人、机构、社会以及国家安全带来的不同影响来确定的该信息系统的安全级别。

20 世纪 50 年代，美军将诞生不久的计算机应用于防空指挥。为了防御其战略对手苏联的核导弹突然袭击，美国又在 60 年代建成集指挥、控制、通信和情报于一体的大型军用计算机信息系统——C^3I 系统（Command、Contro1、Communication、Intelligence）。由于美军最早认识到计算机信息系统在国家安全方面举足轻重的地位，1970 年美国国防科学委员会提出要制定一个关于军用计算机信息系统的安全评价标准，以此来**统一衡量**重要信息系统的安全工程质量，从而使得最高决策部门对这些信息系统的安全状况做到心中有数。此项工作由美国国防部牵头组织实施，历时十余年，于 1985 年 12 月正式公布，名为“可信计算机系统评价准则”（TCSEC，Trusted Computer System Evaluation Criteria），也就是俗称的“橙皮书”。该准则是全球计算机系统安全评估的第一个正式标准，具有划时代的意义。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 首次采用了分级保护的思想，利用**可信计算基**（TCB，Trusted Computing Base）作为建筑安全可靠的计算机系统的“基石”，将计算机信息系统的安全划分为 4 个等级、7 个级别。有兴趣的读者可以在 Google 等搜索引擎上输入 TCSEC DOD 85 等关键字，就可以方便地获得这个计算机信息系统安全等级保护家族的“老古董”文档。表 2.1 简单描述了 TCSEC 各个安全级别的主要内容。

表 2.1　TCSEC 各个安全级别的主要内容

安全等级		详 细 描 述	典型系统示例
D 级	D1	D 类安全等级只包括 D1 一个级别，是 TCSEC 标准中安全等级最低的一级。D1 级计算机系统是完全不可信的，它只为文件和用户提供安全保护，任何人均可无障碍使用	■ 未设置用户登录口令的终端 ■ 未设置安全控制机制的无线网络或者是一个完全没有保护的网络 ■ Internet ■ 早期的操作系统如 MS-DOS 等
C 级	C1	C1 系统的 TCB 通过将用户和数据分开来达到安全的目的，即 C1 系统开始具有一定的可信性。C1 系统要求软、硬件具有一定的访问控制能力 C1 系统不足之处在于用户可直接访问操作系统的根目录，使得用户可以将数据任意移走	■ 机箱加锁 ■ 用户登录口令 ■ 系统管理员可对程序和数据设置访问权限 ■ 系统管理员未设置用户访问权限和级别 ■ UNIX 系统
	C2	在保留了 C1 系统安全机制的情况下，C2 系统加强了安全控制功能。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制能力	■ 管理员可设置用户权限和访问级别 ■ 增加了系统安全审计功能，能够跟踪“登录成功或失败”等安全事件 ■ 企事业机构的门户网站 ■ Windows NT4.0/2000/XP
B 级	B1	B1 系统满足下列要求：系统对网络控制下的每个对象都进行敏感度标记；系统使用敏感度标记作为所有强迫访问控制的基础；系统在把导入的、非标记的对象放入系统前标记它们；灵敏度标记必须准确地表示其所联系的对象的安全级别；当系统管理员创建系统或者增加新的通信通道或 I/O 设备时，管理员必须指定每个通信通道和 I/O 设备是单级还是多级，并且管理员只能手工改变指定设置；单级设备并不保持传输信息的敏感度级别；所有直接面向用户位置的输出（无论是虚拟的还是物理的）都必须产生标记来指示关于输出对象的敏感度；系统必须使用用户的口令或证明来决定用户的安全访问级别；系统必须通过审计来记录未授权访问的企图	■ 对保护对象可以进行敏感度分级标识，如秘密级、机密级和绝密级等 ■ 开始具有强制审计功能 ■ 企事业单位的办公内网（Intranet）

续表

安全等级		详 细 描 述	典型系统示例
B 级	B2	B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的 TCB B2 系统必须满足下列要求：系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变；只有用户能够在可信任通信路径中进行初始化通信；TCB 能够支持独立的操作者和管理员	■ 给设备（终端、工作站、磁盘机等）分配安全级别，如指定用户可以访问一个工作站，但不允许访问装有人事档案信息或工资等私密信息的磁盘子系统
	B3	B3 系统必须符合 B2 系统的所有安全需求，且具有很强的监视委托管理访问能力和抗干扰能力 B3 系统必须设有安全管理员并应满足以下要求：除了控制对个别对象的访问外，B3 必须产生一个可读的安全列表；每个被命名的对象提供对该对象没有访问权的用户列表说明；B3 系统在进行任何操作前，要求用户进行身份验证；B3 系统验证每个用户，同时还会发送一个取消访问的审计跟踪消息；设计者必须正确区分可信任的通信路径和其他路径；TCB 为每一个被命名的对象建立安全审计跟踪路径；TCB 支持独立的安全管理	■ 采用硬件来保护安全系统的存储区 ■ 用数字证书来验证用户身份以及使用权限
A 级	A1	A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求 A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范 A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型，所有的安装操作都必须由系统管理员进行，系统管理员进行的每一步安装操作都必须有正式文档	■ 进行形式化安全验证的系统 ■ 进行产、销、用一条龙的安全跟踪，如一个芯片或磁盘存储子系统从生产、销售到使用都被严密地跟踪

如果读者觉得上述对 TCSEC 的描述比较难于理解，那么下面简单地归纳一下其基本思想：

（1）**基础**，可信计算基（TCB）是构建安全大厦的基石。然后在 TCB 的基础上逐步构建信息系统整体的安全，这也是西方文化“至底向上”、“局部之和等于整体”的系统工程思想的体现。

（2）**粒度**，每一个安全级别都继承了上一个级别的所有安全机制，并逐步增强，因此安全控制粒度越来越细。

（3）**费效比**，安全级别逐步增强的同时，安全代价也快速提高。因此在确定安全级别的时候，需要认真分析信息系统所保护的核心资产（Asset）、面临的安全威胁和相应的系统漏洞（详见本书后半部分“风险评估”相关章节），这样才能产生较好的“费效比”。

2.1.2　中国的计算机安全等级保护标准

中国计算机事业起步于 1956 年，与美国一样，主要为国防事业服务。20 世纪 80 年代之后，中国计算机系统的应用范围也开始大规模从国防领域向民用领域延伸。公安部等有关部门开始了对国外计算机安全标准，特别是对美军“橙皮书”的跟踪研究。1999 年，中国正式颁布了国家标准《计算机信息系统安全保护等级划分准则》（GB 17859）。近年来，随着信息化建设和应用范围的逐步扩展，中国加快了对计算机信息系统和相关安全产品标准制定的步伐，到本书出版时为止，已经初步形成了一个由上百个国家标准和行业标准组成的庞大体系，涵盖了计算机信息系统安全以及各类计算机安全产品等领域。2007 年，全国信息安全标准化委员会正式下达了公安部牵头制定的**《信息系统安全保护等级定级指南》、《信息系统安全等级保护实施指南》、《信息系统安全等级保护基本要求》**等系列标准（截至本书出版为止，这批标准处于“报批稿”状态。——作者注），按计算机信息系统遭受破坏后给个人、机构、社会和国家带来的不同影响程度，将信息系统安全等级划分为 5 个不同的安全级别。

第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第 3 级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级：信息系统受到破坏后，会对国家安全造成特别严重的损害。

信息系统安全等级影响示意如图 2.1 所示。

值得注意的是，在中国 1999 年颁布实施的 GB 17859 等标准中，对信息系统的定级沿袭了美国 TESEC 标准“技术分级”的思想，在实施过程中比较烦琐。而现在所采用的定级指南，则根据“系统遭受毁坏后带来的影响”进行分级，直观、简单、易于操作。

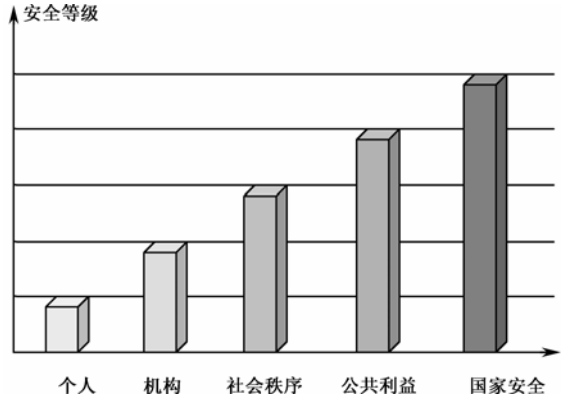


图 2.1　信息系统安全等级影响示意图

从 2003 年开始，中国公安部就开始在全国范围内组织信息安全等级保护试点，并取得了初步的进展。2006 年，中国加大了对信息安全等级保护试点的类型和范围，对信息系统安全等级保护的内在规律有了更为深刻的认识。从 2007 年开始，中国重要信息系统安全等级保护工作已经在全国范围内全面展开。顺便说明的是，第五级信息系统的安全测评工作由国家主管部门负责，不在本书介绍的范围之内。

尽管按照上述定级指南对信息系统进行分级的时候比较容易操作，但相信读者也已经注意到了，如果仅仅按照上面这些文字性的描述，或者说定性的描述，作为一名信息安全测评工程师是无法进行准确、科学的安全测评的（我们总不能故意损坏一个信息系统，然后观察它给个人、社会甚至国家安全带来什么样的影响吧？建议有这种冲动的读者阅读本书“法律、法规”一章）。事实上，国家有关标准对每一级别的信息系统均作了详细的测评要求，我们称为“**测评项**”或“**测评指标**”。第 3 章至第 7 章将结合具体案例介绍测评项。这些测评项覆盖了安全管理、安全技术等不同的领域。这些测评项组成的一个测评集合，是每一个确定安全等级的信息系统应该达到的安全基线（baseline）。因此，一名信息安全测评工程师需要按照国家标准中的各个测评项对一个信息系统进行逐项检查，这就是第 1 章提到的“贯标”。

2.1.3　安全域

与信息安全等级保护密切相关的一个概念是“**安全域**”。安全域是将一个大型信息系统中具有某种相似性的子系统“聚集”在一起。目前，中国划分安全域的方法归纳起来大致有资产价值相似性安全域、业务应用相似性安全域、安全需求相似性安全域和安全威胁相似性安全域 4 种。

资产价值相似性安全域（security zones with similar information assets），指同一安全区域内的信息资产应具有相近的资产价值。

例如，一个信息系统的数据中心往往是该系统最重要的子系统之一，各类数据服务器具有类似的资产价值，可以将它们划入同一个安全域。

业务应用相似性安全域（security zones with similar business applications），指同一安全区域内信息系统的业务应用或系统功能相似。

例如，一个银行的各个支行，其信息系统的业务应用均非常相似，也可以将其划入同一个（纵向广域）安全域。

安全需求相似性安全域（security zones with similar security requirements），指同一安全区域内的信息资产应具有相似的机密性要求、完整性要求和可用性要求。

例如，国家重要政府部门的办公系统，在安全需求方面具有相似性，也可以将其划入一个（横向广域）安全域。

安全威胁相似性安全域（security zones with similar security threats），指同一安全区域内的信息资产应处在相似的风险环境中，面临相似的威胁。

例如，各个企事业单位的门户网站均面临来自 Internet 的安全威胁，可以将其划入一个独立的安全域。



按照**相似性**来划分安全域具有显而易见的优点，例如：

（1）同一套安全防护设备可以保护安全域中的各个子系统，从而节约安全投入的成本。

（2）同一个安全域内的各个子系统可以充分地发挥互联互通、信息资源共享的优点。

（3）不同的安全域之间可以形成多层次配置、纵深防御的安全体系，等等。

需要说明的是，目前人们划分安全域的最主要、也是最常见的方式是将具有相同安全级别的子系统放置于同一个安全域中。当然，不同级别的安全域之间如何进行有效的互联互通等问题依然是进行信息安全等级保护工作中研究的重点之一。

本书将从第 3 章开始，以第 3 级信息系统（以及相应的安全域）为例，向读者介绍整个信息系统安全测评过程，通过学习，读者可以举一反三，把握其他级别的安全测评思想。

与信息安全等级保护密切相关的另外一类标准是信息安全风险评估标准。对这类标准，为保持本书的逻辑性和分类介绍的思想，将放在后面进行专门介绍。这里只是提醒读者注意，信息安全等级保护与信息安全风险评估的内在联系非常紧密。信息安全等级保护是中国信息安全保障工作必须遵循的基本制度，风险评估是实现信息安全等级保护的重要手段。因此从事信息安全测评的人员对这两类标准体系都应该非常熟悉。

顺便指出，国内外涉及国家秘密的信息系统也有相应的分级保护标准和风险评估标准。中国负责制定该类标准的机构是国家保密技术研究所（www.gbms.net.cn），从事相关信息系统安全测评的人员必须遵循这类特定标准。

下面给出信息安全测评的定义。



信息安全测评（testing and assessment of information security），指测评人员在系统工程思想的指导下，遵照国家有关标准、规范和流程，通过设计各种测评案例，对一个信息系统的安全性能和功能进行“标准符合性”论证的过程。

测评过程中我们主要关心的问题是：

（1）系统设计方案是否遵循国家有关标准；

（2）系统设计方案是否得到严格的执行；

（3）系统建成后是否达到设计方案的要求；

（4）系统是否出现方案中未指明的错误，等等。

对上述问题的回答进一步升华之后，就凝练成了信息安全管理体系（ISMS）的思想精髓（参见本书最后一章）。

2.2　何时测评

为了理解隐藏在“何时测评”这个问题背后的真实含义，先请教读者另外一个问题：人什么时候应该接受健康检查？您的答案可能有多种，包括小时候种牛痘疫苗（事前预防），生病后去医院体检（事后补救），上大学之前的体检、年度例行体检，等等。这些答案都对，只不过从完整、科学的角度来回答，我们认为应该是以下四个阶段：

（1）**孕育阶段**：当您的母亲带着幸福而又羞涩的口吻对您的父亲讲，您已经准备加入这个家庭的时候，您的父亲可能（也是应该）要做的第一件事是什么？去医院检查！

（2）**出生阶段**：当您大吵大闹来到这个世界的那一刻，医生护士会马上给您做一个体检。

（3）**成长阶段**：接下来就是常态性和非常态性的各种体检，包括上学期间的体检，工作之后的年度体检，生病之后进行的专项体检……毫无疑问，这个阶段持续时间最长。

（4）**死亡阶段**：无论是谁，都迟早会走到人生的终点。这个时候医生将负责对他/她做最后一次检查，确认他/她已经“潇洒地走了一回”这个叫地球的星球。

读者也许已经猜测到了问题的答案。对一个信息系统进行安全测评，也是贯穿它整个“生命周期”全过程的。这里可以把它分为以下四个阶段。

（1）**设计阶段**：当规划、设计一个信息系统的时候，安全测评工程师应当积极参与规划设计部门的工作，根据国家有关标准，特别是根据信息系统安全等级保护标准对这个信息系统的重要性提出安全评估意见，如可以针对这个系统的重要性（即它遭受破坏

后带来的影响）来事先确定它的安全等级。

（2）**建设阶段**：当这个信息系统的设计蓝图通过有关部门的评审之后，安全测评工程师应当监督该系统的建设过程是否满足国家有关标准。更为重要的是，在系统建设完成之后，应当根据国家标准对其是否达到建设目标进行测评验收。例如，一个信息系统当初设计的时候是按照第 3 级安全标准进行建设的，那么进行验收时就应该按照这个等级进行测评验收。

（3）**运行维护阶段**：经过测评验收之后，系统进入正式运行维护（简称运维）阶段。安全测评工程师将定期或不定期地对系统进行例行测评。这一阶段相对较长（如同人的生长过程），而且往往伴随着系统内部功能的不断延伸和完善，所以需要进行常态性的测评，并且在系统发生安全事故的时候进行及时响应（参见本书“应急响应”一章）。

（4）**废弃阶段**：当该系统确实不堪所用的时候，安全测评工程师需要对它进行最后的测评。读者可能会认为这个环节多此一举。那么请设想一下这种情况吧：一个企业至关重要的商业秘密是否需要按照特定规程进行转移或销毁？当然，这个环节对事关国家安全的重要信息系统更为重要，在信息时代，其重要性甚至不亚于对退役核导弹和核废料的处理，只不过没有那么危险而已。

2.3　测评什么

可以继续采用 2.2 节的比喻来理解这个问题。男人和女人、儿童和成人都需要体检。但其中有什么不同呢？毫无疑问，一个人的生理特征，年龄阶段等决定了体检的项目既有共性，也有差异，对有些从事特殊行业的人体检要求更高，如杨利伟和“许三多”等。



在西方国家，事关国家安全的信息系统也往往采用与 Internet 物理隔离的方法。2001 年“中美撞机事件”之后，中美民间黑客大战给双方的信息系统都带来了一些损失，但美国方面受损的主要是一些政府网页，而非核心系统。需要指出的是，除非双方已经处于敌对交战状态，否则这些“隔靴搔痒”式的鲁莽自发的活动都将受到国际法和国内有关法律的管制。

本书所涉及的信息系统是指那些具有专业用途的网络（恐怕没人愿意去测评 Internet 吧），这里主要指中国各企事业单位的专用网络，如政府、金融、银行、交通、医疗、能源、学校、企业等开展业务工作时所使用的网络。即使是这类专用网络，它们的用途和种类也是千差万别，如果要详细分类介绍，其篇幅和工作量恐怕不亚于当初达尔文那本让“上帝很生气，问题很严重”的名著《物种起源》。因此，根据中国信息化建设现阶段的实际情况并考虑到本书的篇幅所限，下面大致按照这些网络与互联网的连接方式将它们划分为两类，内网和外网。在本书中，**内网**是指那些与 Internet（**公网**）之间采取了**“可靠的技术隔离手段”**的企事

业机构专用网络，如政府内部办公网络、银行内部 OA 系统、企业财务信息系统等。这里的“可靠的技术隔离手段”在目前往往是指与互联网的物理隔离。当然，随着安全防护技术的进步，也有一些在保证安全的前提下方便应用的技术手段出现。为了便于记忆，可以把内网与“3 级以及 3 级以上网络”画等号；**外网**是指那些与 Internet 相连（应该有一定的安全防护措施）并向外提供服务的企事业机构的专用网络。例如，政府对外服务系统、政府门户网站、网络银行、社保网和校园网等。

下面就内网和外网测评的特点做一个简单的比较。详细内容将在后面各章逐步展开描述。

2.3.1　外网测评特点

如图 2.2 所示，一个外网最主要的特点就是与 Internet 相连接，当然这种连接之间存在某种安全保护机制，最常见的就是在外网与公网之间设置防火墙等安全设备并形成所谓的“非军事区”（DMZ）。

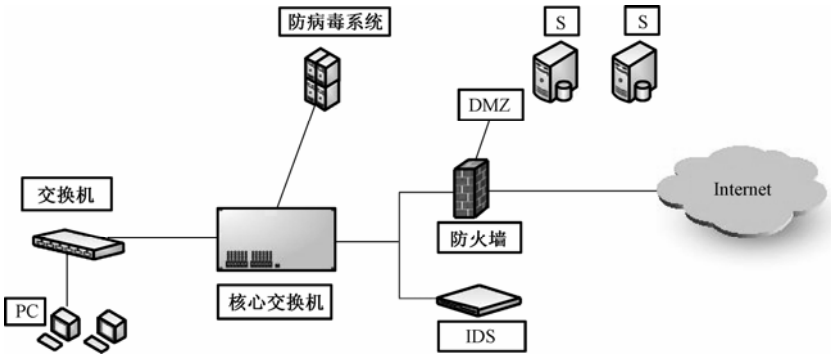


图 2.2　网络边界防御示意图

外网中的防病毒系统可以通过防火墙的配置进行实时的病毒库升级，并将升级之后的防病毒软件分发给外网中的各种服务器（S）或终端（PC）等。

外网安全测评中需要注意以下几个方面问题：

（1）外网安全模型测评。外网安全模型扮演双重角色，一方面它要保护内网。在这种情况下外网“认为”内网是安全可靠的，所以它的主要职责就是防止公网（即 Internet）上的各种安全攻击，并将它作为“跳板”去威胁内网。所以此时测评的重点是外网（或者其子系统）抵御 Internet 上各种安全攻击的能力和水平。另一方面外网的主要功能是向外提供服务，如政府门户网站的公共服务信息，网络银行向用户提供的各种金融服务等。这种情况下外网测评重点是如何保证自身提供服务的连续性。因此，对外网安全等级的测评侧重点分为**对内保护**和**对外服务**两个方面。

（2）外网安全技术测评。按照国家标准，特别是《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评准则》等对外网中各种型号的安全设备、服务器、网

络设备和终端进行技术测评。

（3）外网安全管理测评。按照上述国家标准对外网的各种管理制度、管理人员和管理机构进行测评。

2.3.2　内网测评特点

如图 2.3 所示，一个机构的信息系统如果属于内网，那么该网与 Internet 采用了某种“更安全”的隔离技术手段。例如，采用可靠的网闸设备或者干脆“断网”。在这个内部网络里面，人们依然需要配置各类常见的网络及终端安全防护设备，如防火墙、入侵检测系统（IDS）、漏洞扫描设备、安全审计系统和防病毒系统等。

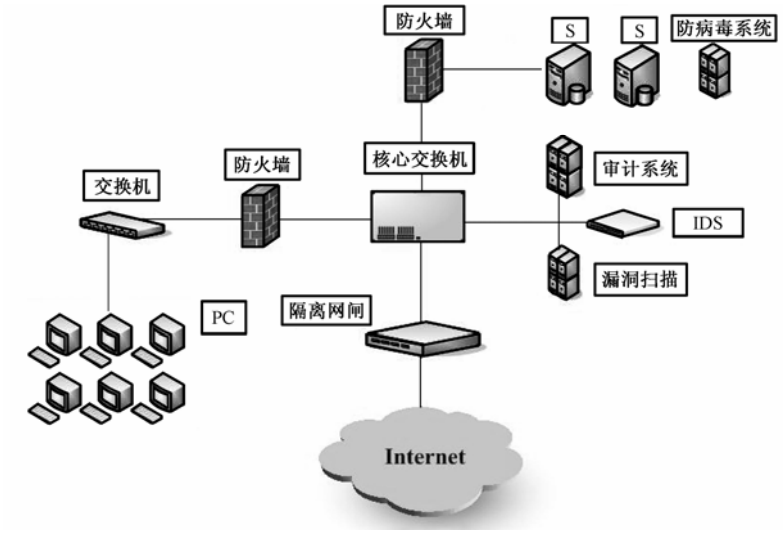


图 2.3　内网拓扑示意图

有的读者可能会感到奇怪，为什么在内网之中还需要采用防火墙、入侵检测系统这类防御外部“黑客”的设备呢？其实人们在内网之中也往往划分了不同安全级别的“安全域”，从而形成多层配置、纵深防御体系。这些安全域之间又构成了“网中网”，所以仍然需要这些安全防护设备。



尽管与 Internet“断网”是内网安全经常采用的方式，但从信息网络发展趋势来看，将来的信息系统必将出现“有线”与“无线”并驾齐驱的局面。例如，美国正在研发的全球网络栅格（GIG）军用通信网络。GIG 体系架构中大量应用了太空通信网络和野战局域网和广域网等。这些均是无线网络，与 Internet 当然是“剪不断理还乱”的关系。它的安全性又将如何保证呢？

一个信息系统通常又分为各种子系统，其中那些支撑一个单位核心业务的子系统是安全保护的重点。例如，各类数据库服务器等。在这类子系统的周边和内部往往有“重兵把守”，配置防火墙、安全审计系统、漏洞扫描系统、防病毒系统等。

需要指出的是，由于内网与 Internet 进行了物理隔离，阻断了公网上各种信息的实时流入以及内网信息的“非授权”流出。但凡事有利则有弊。内网中的各种设备，特别是漏洞扫描设备、防病毒系统等经常需要进行软件升级，如漏洞库和病毒库升级等。对此需要采用特殊的方式，如在与 Internet 连接的终端上对所需的软件刻录成光盘，然后再用光盘“摆渡”到内网之中进行升级。读者可以想象，这种方式其实更多的是依靠健全的安全管理制度和对制度的严格执行而保驾的，而非什么高深的安全技术，所以人们常常讲信息安全是“**管理与技术并重**”。

综上所述，在内网安全测评中需要注意以下 3 个问题：

（1）内网安全模型测评。对内网及其各个子系统的安全设计方案和建设、运行维护情况进行“符合性”测评。该项工作的重点是测评各个子系统或安全域的等级划分是否符合国家有关标准要求和设计要求。

（2）内网安全技术测评。按照国家标准对内网中各种型号的安全设备、服务器、网络设备和终端进行技术测评。

（3）内网安全管理测评。按照国家标准对内网的各种管理制度、管理人员和管理机构进行测评。

2.4　谁来测评

让我们继续沿用健康体检的例子吧。设想一个人感到自己身体不适，那么他/她可能有两种方法来确诊。最常见的一种方式就是去医院看医生（专业诊断），还有一个是自己查看医书或参考以往自己的病历（自诊断）。这两种方式其实都体现了目前中国信息安全测评队伍的组成形式。第一种是所谓的“**委托测评**”形式，由专业的信息安全测评人员组成。第二种是所谓的“**自测评**”形式，主要人员由本单位的技术人员组成（如本单位信息中心的人员）。需要向读者指出的是，根据国家有关部门的要求，目前中国信息系统安全等级保护测评工作的形式是“委托测评”，即由国家主管部门认证认可或授权的第三方专业技术机构进行测评，而信息安全风险评估则既可以采用“委托评估”方法，也可以采用“自评估”方法。本书介绍的重点均是“委托测评/评估”方法。

委托测评队伍

一个病人如果不得不选择医院的时候，有一个因素很重要，那就是选择这个医院的资质。同样的道理，国内外对专业从事信息安全测评的机构也有严格的资质认定。中国负责有关资质审核的权威机构是“中国合格评定国家认可委员会”（www.cnal.org.cn）。该机构根据有关质量体系的标准（如 ISO 9000 等），对从事信息安全测评的机构进行认证。图 2.4 是中国信息安全测评机构的架构图。

专业测评机构的主要优点是：

（1）由于通过了国家或相关主管行业部门的认可，所出具的测评报告具有权威性。

（2）在信息安全技术领域造诣较高，能够及时跟踪并解决复杂的安全问题。

（3）国家或主管行业部门通过专业的测评机构进行的测评工作，可以对整体的安全防护能力有一个可靠、清晰、统一的掌握。

目前，中国专业测评机构也存在一些问题。例如：

（1）由于组建时间较短，在人力资源上尚不能完全保证全国范围内需要测评的信息系统能够及时得以测评。

（2）对于一般的安全事故（也就是对国家或社会影响不大，但对某企事业单位有较大影响）的响应不能“如君所愿”。



图 2.4　中国信息安全测评机构架构图

（3）专业测评机构的建设周期较长，花费较大等。

2.5　如何准备测评

再次引用看病的例子。试想病人到医院看病，需要办理什么手续？先是挂号，然后在正式就医之前，医生要在病历表上填写您的个人信息，为您制定初步的治疗方案等。

同样的，在对一个信息系统进行测评之前，测评人员要进行以下准备工作（见图 2.5）。这是保证整个测评工作质量必要的“繁文缛节”，所以请读者少安毋燥，耐心读下去。

（1）用户（指被测单位）向测评机构提交测评申请书（表）这个过程相当于“到医院挂号”并填写“病例表”。测评机构对用户提交的资料进行初步审核之后，决定是否接受其的测评申请。在此需要说明的是，在实际工作中，测评机构对用户的申请并非总是“有求必应”。例如，测评机构初步分析了用户提交的申请后得出结论，该系统远远达不到国家所规定的等级要求，应该实事求是地告诉用户方尽快进行必要的调整之后再申请测评。表 2.2 是测评申请表的一个模板，谨供参考。

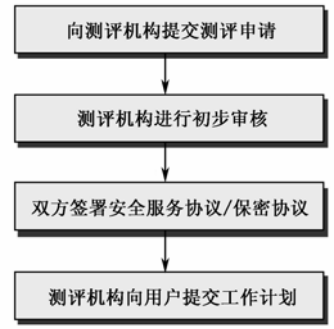


图 2.5　信息安全测评工作流程

表 2.2　测评申请表模板

<table>
<tr><td rowspan="2">申请单位基本信息</td><td>单位（部门）名称</td><td>上级主管部门名称/法人代表姓名</td><td>信息系统应用领域（电子政务、商务、企业等）</td><td>单位授权人姓名及联系方式（电话、邮件地址等）</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">受理单位审批意见</td><td colspan="4">由测评机构负责人或授权代表简述是否受理的意见</td></tr>
<tr><td colspan="2">受理人签字</td><td colspan="2">年　　月　　日</td></tr>
</table>

（2）测评机构对资料进行必要的审核之后，与用户签署安全服务协议书（合同）。该协议书对甲乙双方的责权利均有明确规定，是保证测评服务质量必备的具有法律效益的文件。

服务协议（SLA，Service Level Agreement），指申请测评的用户（甲方）与测评机构（乙方）签署的具有法律效益的文件。SLA 规定了甲乙双方在此次测评活动中的责任、权利和义务。

错误！

××信息系统安全服务协议书

签约方

甲方：××机构（被测单位名称）

乙方：××信息安全测评机构

协议书内容

第一条　项目名称

第二条　项目目标

第三条　项目内容

第四条　甲方义务

第五条　乙方义务

第六条　违约责任

第七条　争议解决办法

第八条　……

甲方代表签字（章）　　乙方代表签字（章）

年　月　日　　年　月　日

（3）与用户签署保密协议书。在看病过程中，您一定不会愿意看到主治医师将您的病情宣传得满世界都知道；另一方面医生（特别是中医）也要保护自己的“祖传秘方”（用时尚的话来讲就是“保护知识产权”）。保密协议书是保护用户业务秘密和测评机构工作秘密的法律文件，对双方均有法律上的约束。

保密协议（Confidential Agreement），指申请测评的用户（甲方）与测评机构（乙方）签署的具有法律效益的文件。保密协议规定了甲乙双方在此次测评活动中保守对方业务、技术和工作等秘密的承诺。

××信息系统安全服务保密协议

甲方：××机构（被测单位名称）

乙方：××信息安全测评机构

甲乙双方根据国家和地方有关法律、法规规定，就本次安全服务工作所涉及的核心业务机密达成如下安全服务保密协议。

合同内容

第一条　保密内容和范围

第二条　双方的权利和义务

第三条　协议有效期

第四条　免责条款

第五条　违约责任及解决办法

第六条　……

甲方代表签字（章）　　乙方代表签字（章）

年　月　日　　年　月　日



在上述保密协议书中，有几点需要做出说明。“保密内容和范围”应当包括被测单位的业务机密、敏感数据（如企业经营数据、财务信息等）等。这方面的内容由甲方提出。此外，还要包括信息安全测评机构的工作秘密，如使用的测试工具和方法等，这方面的内容由测评机构提出。“免责条款”主要是指测评双方业已公开的各种信息不在保密条款之内。当然，也可以将“信息安全服务协议”与“信息安全服务保密协议”合二为一。

（4）向用户提交测评工作计划。

××信息安全测评机构

××信息系统安全服务工作计划

第一章　工作目标
第二章　工作范围
第三章　工作重点
第四章　进度安排
第五章　保障措施
第六章　约束条件
第七章　计划审批
第八章　……
附录 A　测评依据
1．国家标准一
2．国家标准二
3．……
附录 B　被测单位与测评单位简介

附录 C　术语及名词缩写

错误！

制定工作计划是保证测评质量必不可少的步骤，也是一个测评机构正规化、标准化服务的重要体现。该工作计划扮演双重角色，既是测评机构承担此次测评任务的工作指导书，同时也应当达到让用户了解测评工作的各个环节的目的，以获得用户对测评机构服务质量的认可。以下是制定工作计划时需要注意的要点：

（1）工作目标。该部分内容主要包括此次测评工作要达到的目标，如对 XX 信息系统第 3 级安全等级保护进行测评。开展此次测评工作的背景等有关情况也可以在此进行描述。

（2）工作范围。该部分内容包括测评对象是什么，即说明系统边界在什么地方。工作的范围和内容要清晰、明确。例如，对测评的各个子网络、应用系统、信息点等要尽量进行量化描述。换言之，对所要测评的系统边界要明确。

（3）工作重点。该部分内容主要是指测评活动的优先级排序。例如，在对一个电子政务系统的安全进行测评时，其政府门户网站与其核心业务系统或数据中心相比，重要性就较低。因此，在安排测评资源时应该按照轻重缓急来安全测评资源（人员和设备等）。

（4）进度安排。明确测评范围和测评重点之后，应该制定一个测评工作时间表，将测评活动的时间节点（milestone）标识出来。使用“甘特图”等方式来表示测评进度是

一个较好的方法。

（5）保障措施。该部分主要是阐述为了保证此次测评活动圆满结束的前提条件，包括甲乙双方的组织关系，如测评队伍的组成、用户单位哪些人员需要配合（如该单位信息中心人员），等等。最为重要的是，在对一个大型复杂的信息系统进行测评时，双方都需要指定一名代表，扮演沟通渠道（communication channel）的角色，保证信息交流的唯一性。

（6）约束条件。该条件在有的工作计划中也称为“风险分析”，即如果出现不可预测的情况时对测评活动有何影响。例如，被测评的信息系统出现重大变化（新增某些大型设备或软件，甚至出现系统搬迁等极端情况）。



政务公开与信息安全。随着信息技术的发展，政府的职能在转变得越来越贴近人民大众，政府的效率正经历着空前的提升。对此做出不可磨灭技术贡献的，就是 Internet 及其相关技术。

Internet 为什么那么强大，影响那么深远？追本溯源，只有两个字——开放。开放带来了最大限度的共享，开放消除了时空障碍，开放彻底改变了人类交流乃至思维的方式和效率。

但是，剑有双刃。开放就得面对风险，面对安全问题。不能因噎废食，不能因为有新的安全问题就回到封闭隔离的状态。如果回归到没有 Internet 的年月，世界将是怎样？

（7）计划审批。这个环节往往是测评活动中容易忽视的。事实上，工作计划必须获得甲乙双方主管负责人（或授权人）的批准之后才能实施。这是质量保证体系中的必要手续（参见本书最后一章）。

（8）测评依据。该部分主要是罗列此次测评活动中所依据的国家标准以及参照的其他相关标准。

（9）术语和名词缩写。由于在测评活动中会产生大量的测评报告（包括工作计划本身），所以在此可以罗列一些常见的缩写和术语，以便于阅读。

我们终于“熬过”了上面这些“八股文”，现在可以开始进入作者和读者都感兴趣的章节了。

2.6　怎样测评

古人云：“临渊羡鱼，不如退而结网”（《汉书 董仲舒传》）。从本节开始，将通过一个贯穿本书第 3 章至第 6 章有关信息安全测评的大型模拟案例，陆续向读者介绍信息安全测评的方方面面。首先，按照测评工程师的“行规”，给这个模拟的信息系统取一个意味深长的代号，以便于本书后面引用。当然，这个代号反映的仅仅是本书作者的偏爱，如果您愿意，也可以把它冠以“快男超女”之类的时尚代号。

汉武帝时代是中国历史上最辉煌的朝代之一，既诞生了卫青、霍去病这些名传千古的军事将领，又孕育了董仲舒、司马迁等这些伟大的思想家。所以我们把这个模拟信息系统称为“天网”如何？“天网恢恢，疏而不漏”。当然，这里并不代表本书作者赞成大儒董仲舒“天人感应”的迷信学说和“废黜百家、独尊儒术”的学术独裁思想。

2.6.1　测评案例——“天网”工程



在好莱坞拍摄的科幻大片“终结者 3”（Terminator 3）中，人类与具有自我意识的病毒系统“天网”（Sky Net）展开了殊死搏斗。关于计算机智能或者计算机网络是否将替代人类的话题一直是科学家和文学家们热议的话题。我们认为，将来的发展趋势可能有两种，一种是人类从事更加智能的工作，而计算机网络则从事辛苦但又相对“弱智”的工作；还有一种是“人–机结合”、“人网结合”的态势，从而引发重新诠释关于生命的定义……

“天网”工程背景：巴山市电子政务信息系统——“天网”集政府内部办公和政府部门之间协同办公（G2G）、政府面向企业服务（G2E）以及政府面向社会公众服务（G2P）等功能于一身。

（1）G2G：“天网”工程 G2G 功能要满足政府内部办公和政府部门之间协同办公业务的需要。一个具体的例子是：为解决巴山市中低收入居民住房困难的情况，该市市长签发了一份关于本市居民“旧房改造工程”的电子公文，这份公文将通过“天网”系统下达到市财政局（政府拨款）、市国土资源局（房屋用地审批）、市社会与劳动保障局（享受此项福利的市民资格审批）、市建设委员会（建设规划审批）、市林业局（住宅小区绿化工程主管部门）等该市政府下属各部门。在本书中，“天网”的 G2G 子系统是一张内网。

（2）G2E：“天网”工程 G2E 的功能要满足政府面向企业服务的需要。一个具体的例子是：假设一家国际著名 IT 企业要入驻该市高新技术开发区。那么该企业将通过“天网”G2E 系统办理相关手续或咨询相关问题，涉及的政府部门可能包括：市工商管理局（办理营业执照）、市地方税务局（办理税收手续并咨询相关的优惠政策）、市信息产业局（主管高新技术）、市公安局（外籍高层管理人士出入境管理）、市教育局（咨询本地大学相关专业学生情况、外籍员工子女入学情况）、海关总署驻本市分支机构（进出口主管部门），等等。

（3）G2P：“天网”工程 G2P 功能要满足政府面向社会公众服务的需要。一个具体的例子是：假设读者向“市长公开信箱”反映“神农半仙”医院医疗就诊收费所存在的问题。那您可以通过“天网”系统所属的政府门户网站直接给市长公开信箱发送邮件。而这个邮件经市长批阅之后，可能又会通过“天网”系统转发给市人大（请示地方立法机构进行调研）、市卫生局（医疗卫生主管部门）、市劳动与社会保障局（主管您的医疗保险费用）、市政府新闻办（负责在政府门户网站上答复您的提问，如果您的提问具有普遍性和代表性的话）等相关部门。

在本书中，“天网”的 G2E、G2P 子系统属于外网。图 2.6 是“天网”系统的网络拓扑图。

综上所述，“天网”系统囊括了一个现代化大型信息系统应用的方方面面。可以想象“天网”一旦瘫痪，对本市的政治、经济、文化和民生等均可能产生较大的影响，因

此“天网”的安全等级被定为第 3 级。按照国家有关规定，“天网”将进行委托式安全测评，经国家有关部门授权的专业测评机构正在为该项测评任务做准备。

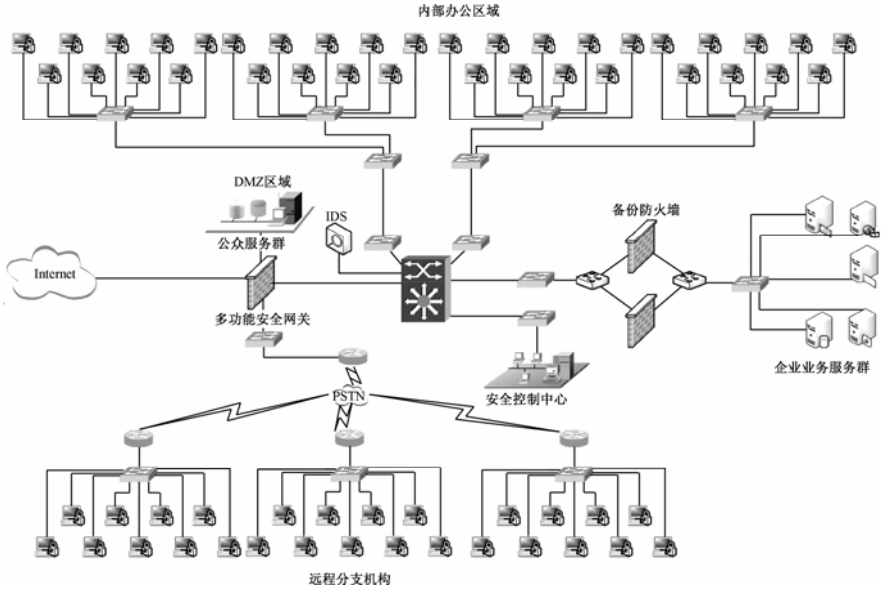


图 2.6　“天网”系统网络拓扑图

2.6.2　启动“天网”测评

现在可以将本章前面所介绍的内容综合在一起“有的放矢”地进行案例练习了。下面假设“天网”已经向一个专业测评机构——“深海”信息安全测评中心提出测评申请并获得该机构的审批，同时双方也签署了相关的 SLA 和保密协议。现在给出“天网”测评工作计划的模板，当然由于篇幅的原因，这里仅仅摘其要点进行介绍。

错误!

“天网”信息安全测评服务工作计划

客户名称：巴山市政府信息中心

计划编制：“深海”信息安全测评中心

文档编号：TW-GZJH-001

更新日期：2008 年 10 月 1 日

错误!

第一章　工作目标

一、根据巴山市政府信息中心的申请，此次测评工作将对巴山市电子政务网络进行测评（起因）。

二、此次测评工作是巴山市全面开展重要信息系统安全等级保护工作的有机组成部分（背景）。

三、巴山市政府组织有关单位和专家组对该市“天网”系统进行定级评审，确定“天网”系统安全等级为第 3 级。

四、此次测评工作的目标将根据国家有关标准，按照第 3 级信息系统的要求进行测评（目的）。

错误!

第二章　工作范围

一、“天网”系统逻辑结构分为网络层、数据层和应用层。

二、“天网”系统由 G2G、G2E 和 G2P 三大分系统组成。

三、G2G 是政府办公内网，与外网进行了物理隔离。G2G 分系统包括以下 10 个子系统（略）。

四、G2E 是政府对企业服务系统，G2P 是政府对公众服务系统，属于“天网”系统的外网。G2E 分系统包括 22 个子系统（略），G2P 分系统包括 14 个子系统（略）。

五、“天网”系统各个子系统安全等级及安全域分级保护列表如下（略）。

错误!

第三章　工作重点

根据“天网”系统分级保护列表，此次测评工作优先级如下：

测评对象	G2G	G2E	G2P
资源分配	★★★★	★★★	★★
测评分工	A 组	B 组	C 组

错误!

第四章　进度安排

测评流程	第一周	…	第 *N* 周
准备阶段			
现场测评			
数据分析			
撰写报告			
结果确认			

错误！

第五章　保障措施

组织保障

一、“深海”信息安全测评中心“天网”信息安全测评服务项目的组织机构图（略）

二、巴山市政府信息化领导小组以及信息中心组织机构图（略）

技术保障

一、“深海”信息安全测评中心下属技术队伍（略）

二、巴山市政府信息中心下属技术队伍（略）

三、“天网”项目双方沟通渠道联系方式（略）

资金保障

……

错误！

第六章　约束条件

项目风险分析

一、风险因素 A 分析及其解决办法

二、风险因素 B 分析及其解决办法

三、……

四、不可预测条件

第 *N* 章　计划审批

甲方：（授权代表签字）　　乙方：（授权代表签字）

2008 年 X 月 X 日

错误！

附录 A　测评依据

《信息安全等级保护测评指南》（GB XXXX）
《信息系统安全等级定级指南》（GB XXXX）
《信息系统安全等级技术要求》（GB XXXX）

附录 B　术语及缩写

“天网”：巴山市电子政务信息系统
G2G：巴山市电子政务内网
……

在完成了测评工作计划的撰写之后，我们将从第 3 章开始根据国家标准分别就“天网”系统的“数据安全”、“主机安全”、“网络安全”、“应用安全”等内容进行测评。

2.7　本章小结

- 信息安全测评 5W+H 的内涵
- 中国信息安全测评的主要标准
- 信息安全等级保护的定级方法
- 安全域的四种划分方法
- 安全域划分的优点
- 信息安全测评的定义
- 信息安全测评与信息系统生命周期的关系
- 内外网安全测评的特点
- 测评机构的组织体系
- 服务协议与保密协议扮演的角色
- 测评工作计划的作用以及制定工作计划所涉及的内容

尾声：比《新工具》更新的是什么？

17 世纪的培根穿过时光隧道，经过 400 年的行程，来到 21 世纪，怀中揣着《新工

具》。

核武器、导弹、宇宙飞船、基因工程、克隆技术、互联网和移动通信都难不倒他，说早该有了。他拿出他的《新工具》搁在桌上，悠然自得地随手翻开本 21 世纪的书，却随即满脸狐疑地问道，TCSEC、GB 17859、BS 7799、ISO/IEC 17799，都是些什么工具啊？

信息时代的新东西层出不穷，尤其在信息技术领域本身，出现新概念、新技术、新术语和新标准，其速度前所未有，让人眼花缭乱。但脉络总是清晰的，那就是，新思想、新概念、新技术、新方法，终成新标准。哦……培根说。

人类作为万物之灵，按照区别于其他动物的本质特征的定义就是能制造工具并使用工具进行劳动的高等动物。所以“工具”是何等重要。

这个时代的工具太多了。往后推 100 年、1000 年，就会更加分明地看到，我们正处于一个前所未有的巨变时代，其特点就是“新工具”层出不穷。所以，作为方法论，还是把“新工具”这个词的专利使用权留给培根吧。

观感

（1）为什么在信息安全测评的时候要强调贯彻国家标准？

（2）请在网上查阅中国有关信息系统和安全产品的标准，如关于操作系统、数据库和防火墙等相关的安全标准。

（3）请在网上查阅美国国家标准技术局（NIST）有关信息安全风险评估的标准。

（4）请在网上查阅美国 TCSEC 标准。

（5）请在网上查阅美国国防部国家安全局（NSA）关于“信息技术保障框架”的资料。

（6）日本、德国、俄罗斯和以色列等国家关于信息系统安全保护的国家标准或政策有哪些？

（7）中国国家标准中关于信息系统定级的出发点是什么？

（8）中国信息安全等级定级与 TCSEC 定级的区别是什么？

（9）安全域划分与信息系统安全定级是什么关系？

（10）一个安全域可否包含不同安全级别的子系统？您的理由是什么？

（11）信息安全测评队伍与通常的信息安全生产厂商技术服务队伍有什么区别？

（12）请登录您所在地区的政府部门网站、大型企业网站或者校园网，并根据收集到的相关资料撰写一份信息安全服务协议、一份信息安全保密协议。

（13）请在第 12 题的基础上撰写一份信息安全测评工作计划。

（14）某省政府门户网站系统“天府之窗”，主要用于发布政务公开信息、地方行政法规和管理措施、领导讲话、政府办事流程、新闻发布、政府公告、举报投诉、省内经济形势介绍、电子表单下载等信息，服务对象主要是省内企业和市民。

①“天府之窗”是省政府对社会办公的窗口，其中发布的信息内容代表政府形象和

体现政府的社会管理和社会服务职能，因此该系统被破坏可能对社会秩序造成一定影响。

② 由于省政府网站的访问量并不很大，信息被篡改可能造成的不良社会影响不会很大，因此对社会秩序的侵害程度为一般损害。

请您根据国家标准对“天府之窗”定级。

（15）某省电力集团公司的省级电力实时监控系统，主要运行调度自动化控制系统和能量管理系统（SCADA/EMS）DDZDH，负责省级超高压输电变电站的调度控制和数据采集。系统实时性要求极高，达到秒级。我们对该系统的分析如下:

① 电力系统是国家重要基础设施，省级 DDZDH 系统负责全省范围内的电力调度，调度控制指令或调度程序被修改，可能造成的停电事故会影响几乎所有行业的正常生产和工作，其所侵害的对象为社会秩序和公共利益。

② 调度控制指令或调度程序被修改可能造成全省范围的大面积停电、人员伤亡和巨额财产损失，同时对其他行业的生产和工作造成非常严重的影响，因此对社会秩序和公共利益的侵害程度为特别严重损害。

请您根据国家标准，对 DDZDH 系统定级。

第 3 章
数据安全测评技术





凯撒大帝银币

弄斧必到班门。

——华罗庚

序幕：谜已解，史可鉴

纵观东西方文明发展史，在信息安全方面往往有着惊人的巧合。

历史画卷之一：3000 年前的特洛伊城下，当数十名希腊特种兵手持利刃鱼贯进入木马腹中的时候，逐鹿中原的周武王与姜子牙正在中军账里探讨军事保密通信的方法。君臣二人一问一答，确定了阴符、阴书等保密通信手段的不同用途（《六韬·龙韬》）……

历史画卷之二：2000 年前，当雄才大略的凯撒大帝在高卢战争中刻苦钻研他首创的“置换密码”的时候，伟大的秦王朝已经在世界上率先建立起庞大的军事保密通信网——驿站……

历史画卷之三：1000 年前，当拜占庭帝国的将军们正在与波斯王朝的大军“鹬蚌相争”的时候，自然不会想到 1000 年后有人会以他们的名义研究信息安全（The Byzantine Generals Problem）。与此同时，被女真人的入侵弄得心神不定的宋朝皇帝赵桓却龙颜大悦。读完了大臣曾公亮“奉旨完书”的《武经总要》之后，老皇帝深深地被这位军事家提出的“五言律诗”加密法所吸引，禁不住亲提御笔为其写序……

历史画卷之四：100 年前，当清朝驻日公使汪凤藻到东京邮电局使用西洋密码给国内发送机要电报的时候，日本电信课长佐藤爱磨正暗暗窃喜，从此也就决定了亚洲最庞大的海军北洋舰队覆灭的命运……

历史画卷之五：60 年前，当剑桥大学高材生图灵在伦敦布莱奇利公园为破译纳粹德国的“隐语”密码（Enigma）冥思苦想的时候，重庆歌乐山下，初中文凭的华罗庚则一眼就看穿了日军利用“莫比乌丝”带（Mobius）加密的小伎俩，让国民政府军政部长俞大维大喜过望……

现实画卷：今天，各国的信息安全工程师们都在忙于保护自己的数据安全，当然也有人忘不了窥视别人的秘密……

无论是过去、现在，还是将来，数据安全始终都是信息安全最本质、最核心的部分。从本章开始，我们将与读者一道探讨如何测评一个信息系统的数据安全。

要点：本章结束之后，读者应当了解和掌握

- 数据安全测评的国家标准是什么？
- 数据安全测评的 3 种手段是什么？
- 怎样进行数据安全测评？

3.1　数据安全测评的诸方面

一个信息系统的数据，就好比存储在银行金库里的金条。对这些在化学元素周期表上排名第 79，但在地球人心目中排名第一的金属，一个金库管理员是怎样确认它的安全的呢？

首先，金库管理员在盘点的时候金条不能少也不能多。如果金条的数量少了，管理员着急；如果金条的数量多了，总会有人着急。其次，金条的数量（甚至金库里储存了些什么）不能让外人知道。最后，需要使用金条的时候能够用得上。这一点也很好理解：假设有人告诉您，他有黄金万两，但就是永远取不出来。您还会相信他，和他多说一句话吗？

对比之下，相信读者已经知道数据安全的三个属性了吧？那就是“**完整性**”（integrity）、“**保密性**”（confidentiality）和“**可用性**”（availability）。因此，在测评一个信息系统的数据安全时，国家标准要求从“数据完整性”、“数据保密性”和“数据备份与恢复”三个环节来考虑。

那么怎样对数据安全进行测评呢？无论中医还是西医，看病时都是灵活运用“望、问、闻、切”这些手段。同样的，国家标准中要求信息安全测评工程师使用访谈（“闻”与“问”）、检查和测试（“望”和“切”）这三种方法进行测评。下面给出“访谈”、“检查”和“测试”的定义。



访谈（interview），指测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。

在访谈过程中，建议测评工程师遵照国家标准并结合该信息系统的实际情况，制定相应的问卷调查表。3.2 节将结合“天网”案例分析给出数据安全问卷调查表的一个模板。



检查（examination），指测评人员通过对测评对象进行观察、查验和分析等活动，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。

检查工作中要求测评工程师对信息系统的有关建设文档资料，各种软、硬件设备和环境进行（现场）检验。例如，信息系统拓扑图的现场比对，数据库管理系统的安全配

置检查，等等。

测试（testing），指测评人员通过对测评对象按照预定的方法/工具使其产生特定的行为等活动，然后查看、分析输出结果，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。

测试过程中往往要求测评工程师利用各类专用工具对信息系统进行渗透性测试。这个过程是充分发挥一个测评工程师艺术创造力的时刻。读者将在下面看到各种测试案例。在此需要特别强调两点：一是本书给出的测试方法仅仅是“抛砖引玉”，相信各位读者会有许许多多更好的方法。二是测试过程一定要注意“无损测试”，也就是不能影响被测系统的正常工作，也不能留下任何后患。

1928 年，苏联提出使用超声波进行无损探伤的概念。无损检测（NDT，Non-Destructive Testing），是指对材料或工件实施一种不损害或不影响其未来使用性能或用途的检测手段，是目前工业界广泛应用的检测技术之一。例如，中国航天发射活动中，对昂贵的长征系列运载火箭、卫星等均必须采用 NDT 的方法进行检测。

信息系统同样也是非常“娇贵”的，在进行测试的过程中也要注意进行无损测试。而如何将其他领域的 NDT 思想应用到信息系统之中，这是一个非常有意思的研究领域。

对数据安全进行测评，实际上就是对“数据完整性”、“数据保密性”和“数据备份和恢复”三个环节，利用访谈、检查和测评三种手段进行科学分析的过程。图 3.1 是数据安全测评的框架图。

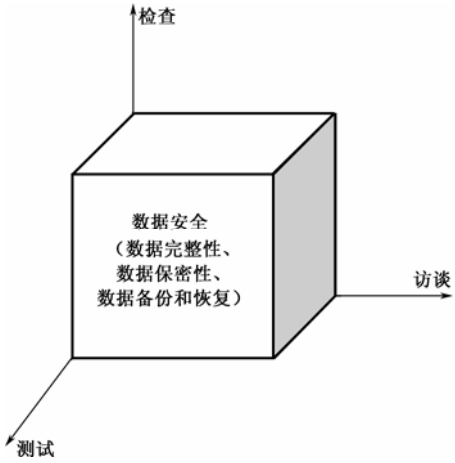


图 3.1　数据安全测评框架图

3.2　数据安全测评的实施

假设“深海”信息安全测评中心已经制定了工作计划（见 2.6.2 节），现在进入了对“天网”系统的数据安全测评阶段。根据第 2 章的介绍，“天网”系统的安全等级为 3 级。为此，需要根据国家制定的第 3 级数据安全标准开始以下测评工作。

首先，需要向初次接触测评工作的读者说明，一个信息系统定为某一级（如第 3 级）是一个“整体定级”的概念。换言之，一个信息系统分为若干子系统，如果其中一个子系统被定为了第 3 级，那么整个信息系统的安全级别就是第 3 级。但这并不意味着它所有的子系统都是第 3 级。因此测评工程师在测评某一个子系统的时候，应该按照这个子系统的实际级别开展测评。

在本章所使用的案例中，假设巴山市电子政务系统“天网”下面有一个社会劳动保障子系统“杜甫”，这是一个面向公众服务的 G2P 子系统。由于它所涉及的是巴山市普通民众“五保合一”（医疗保险、失业保险、养老保险、工伤保险、生育保险等）的切身利益，一旦发生安全事故必将给巴山市的社会稳定带来较大影响。所以将“杜甫”定为第 3 级。而在这个第 3 级子系统中，尽管网络中断会带来不利的影响，但根据社保工作的特点，一般认为网络中断一天左右尚属于可以“容忍的”范围。关键是“杜甫”的数据库子系统不能发生被篡改、长时间不可用及公民个人隐私不能外泄等安全事件。因此，下面将依据国家有关标准中对数据安全第 3 级的要求，对“杜甫”子系统的数据安全进行测评。也许有的读者会觉得下面介绍的测评细节非常烦琐，但请读者注意，这就是测评贯标的思想，也是测评工程师的高价值所在。为了叙述简洁，本书中一律将“信息系统安全等级保护基本要求”中的第 3 级要求称为“第 3 级安全测评要求”，特此说明。

3.2.1　数据安全访谈调研

数据安全访谈调研过程主要是测评工程师与被测信息系统的各级管理人员、技术人员和数据使用人员进行问卷式的访谈。访谈的内容分为数据完整性、数据保密性及数据备份和恢复三大块。首先介绍国家标准中关于数据完整性、保密性和备份与恢复三个方面的访谈要求，然后通过一个访谈问卷调查表的形式来细化访谈内容。

1．数据完整性访谈

在第 3 级安全测评要求中，数据完整性访谈只有 1 项。

应访谈安全管理员，询问主要应用系统数据在存储、传输过程中是否有完整性保证措施，具体措施有哪些；在检测到完整性错误时是否能恢复，恢复措施有哪些，等等。

2．数据保密性访谈

在第 3 级安全测评要求中，数据保密性访谈一共有 5 项。

（1）应访谈网络管理员，询问信息系统中的主要网络设备的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性。

（2）应访谈系统管理员，询问信息系统中的主要操作系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性。

（3）应访谈数据库管理员，询问信息系统中的主要数据库管理系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性。

（4）应访谈安全管理员，询问信息系统中的主要应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性；是否采用加密或其他保护措施实现存储保密性。

（5）应访谈安全管理员，询问当使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息。

3．数据备份与恢复访谈

在第 3 级安全测评要求中，数据备份与恢复访谈一共有 4 项。

（1）应访谈网络管理员，询问信息系统中的主要网络设备是否提供本地数据备份与恢复功能，完全数据备份是否每天一次；备份介质是否场外存放；是否提供利用通信网络将关键数据定时批量传送的异地数据备份功能；是否不存在关键节点的单点故障；关键网络设备、通信线路和数据处理系统是否具有高可用性。

（2）应访谈系统管理员，询问信息系统中的主要主机操作系统是否提供本地数据备份与恢复功能，完全数据备份是否每天一次；备份介质是否场外存放。

（3）应访谈数据库管理员，询问信息系统中的主要数据库管理系统是否提供本地数据备份与恢复功能，完全数据备份是否每天一次；备份介质是否场外存放。

（4）应访谈安全管理员，询问信息系统中的主要应用系统是否提供本地数据备份与恢复功能，完全数据备份是否每天一次；备份介质是否场外存放。

如上所述，国家有关第 3 级安全的测评要求中规定的数据安全的访谈项共有 10 项。初次接触这个领域的读者如果“照本宣科”去开展访谈工作，可能会不知道从何下手。为此我们设计了一个访谈问卷调查表模板（见表 3.1），供不熟悉这部分内容的读者参考。当然，在实际工作中读者应该根据自身工作的特点来制定您所需的访谈记录表。

问卷调查表的设计

为了帮助读者了解问卷调查表应该包含那些内容，下面介绍一下问卷调查表的设计

思想。如上所述，国家有关信息系统安全等级保护测评要求中所涉及的问卷调查内容分为三大部分：数据完整性访谈、数据保密性访谈及数据备份和恢复访谈。因此，在设计问卷调查表的时候就应当分为这三大类进行访谈调研。

在进行数据完整性访谈调研时，访谈的重点应包括操作系统、数据库，可能影响数据完整性的各种软、硬件设备及人为或自然灾害等情况。而访谈的对象则包括系统的安全管理人员和数据使用者等。

在进行数据保密性访谈调研时，访谈的重点除了上述访谈中所覆盖的内容之外，还增加了有关业务敏感性数据的访谈调研，如财务系统、OA 系统、审计系统、邮件系统等。此外，各种安全防护设备的情况也是进行调研的重点。访谈的对象则包括数据库管理员、网络管理员、系统管理员等。

在进行数据备份和恢复访谈调研时，访谈的重点又增加了有关备份机制、制度、相关设备等方面的内容。访谈对象依然是系统或网络管理人员。

这里要提醒读者注意的是，设计问卷调查表中的每一个细节均是可“裁剪”的，即读者应根据自己在访谈调研的具体情况进行增减。同时，有许多访谈项既是在调研数据完整性所希望知道的，也可能是数据保密性或数据备份和恢复所需要了解的。因此要尽量避免重复提问，或者尽量做到“一问多答”。


使用问卷调查表的好处是多方面的，例如：

（1）可以提前将这类调查表寄给被测信息系统的管理和技术人员，让他们事先进行相关问题的准备，从而避免“漫无目的”的问答现象。

（2）问卷调查表是测评工作记录之一，它将国家有关标准进行了细化，操作起来比较方便，有利于在后期撰写测评报告时进行分析。

（3）在现场访谈调研的时候，往往需要边问边记，如果您没有接受速记员的训练，很可能会手忙脚乱，缺一漏十。而使用录音设备等方式又会给被访谈对象一种“受审查”的不良感觉。所以按照事先设计好的表格和方框，根据用户的答案在方框选项中打“√”，效果可能要更好一些。

测评人员在进行访谈调研时，还有一点需要注意，那就是涉及到被测系统所发生的各种安全事件这类敏感话题时，由于可能牵涉到责任的认定或本单位的形象，所以被访谈的人员有时会产生防范心理。因此如何营造一个“畅所欲言”的访谈环境，让被询问人员认同您所以需要了解这些情况，是为了更好的给他们提供安全服务的观点。这项工作有点类似于遭受天灾之后进行“心理疏导”，每一位访谈调研人员需要在工作中不断积累这种工作技巧。当然，测评人员也要向访谈对象声明，这些访谈内容均受到双方签署的保密协议的约束，以进一步打消他们的顾虑。表 3.1 是根据国家有关标准细化整理的访谈问卷调研表，仅供读者参考。

表 3.1　数据安全测评访谈问卷调查表

访谈类型	设 备 型 号	访 谈 内 容	访谈对象	备注
数据 完整性	操作系统版本	应用系统数据完整性表现形式	□ 安全管理员 □ 技术员 □ 数据使用人员	
	□ Windows 2000/XP/ VISTA □ UNIX □ Linux Red Hat/红旗 Linux □ 其他（请注明）	（1）硬件完整 □ 磁盘无故障 □ 电源无故障 □ 存储器无故障 □ 介质、设备和其他备份无故障 □ 芯片和主板无故障 □ 其他 （2）网络完整 □ 保证 网络服务器上的 网络接口不出故障 □ 网络布线设计的抗压力大 □ 采用屏蔽双绞线或光纤系统进行 网络的布线防电磁辐射		
		（3）逻辑完整 □ 软件无错误 □ 文件无损坏 □ 数据交换无错误 □ 容量无错误 □ 操作系统无错误 □ 其他 （4）意外的灾难事件 □ 自然灾害 □ 工业事故 □ 蓄意破坏/恐怖活动 □ 其他 （5）人为因素 □ 无意外事故 □ 经验丰富 □ 无压力/恐慌 □ 通信顺畅 □ 无蓄意的破坏和窃取 □ 其他		
		恢复数据完整性和防止数据完整性丧失		

		□ 备份 □ 镜像技术 □ 归档 □ 转储 □ 分级存储管理 □ 奇偶检验 □ 灾难恢复计划 □ 故障发生前的预前分析 □ 电源调节系统 □ 系统安全程序 □ 其他		

续表

访谈类型	设 备 型 号	访 谈 内 容	访谈对象	备注
数据完整性	数据库版本	数据库数据的完整性		
	□ Oracle □ SQL □ 其他	□ 实体完整性措施 □ 参照完整性措施 □ 用户定义的完整性措施 □ 完整性约束命名字句 □ 域中的完整性限制 □ 触发器控制 □ 其他		
数据保密性	网络设备	网络数据保密性	□ 网络管理员 □ 系统管理员 □ 数据库管理员 □ 安全管理员	
	□ 防火墙 □ 路由器 □ 交换机 □ UPS □ VPN 设备 □ 其他	□ 网络设备的鉴别信息加密 □ 敏感的系统管理数据加密 □ 敏感的用户数据加密 □ 网络传输加密措施 □ 其他		
	操作系统版本	系统数据保密性	□ 网络管理员 □ 系统管理员 □ 数据库管理员 □ 安全管理员	
	□ Windows 2000/XP/VISTA □ UNIX □ Linux Red Hat/红旗 Linux □ 其他（请注明）	□ 操作系统提供本地数据备份与恢复 □ 每天备份与恢复功能 □ 备份介质场外存放 □ 其他		
	数据库版本	数据库数据保密性	□ 网络管理员 □ 系统管理员 □ 数据库管理员 □ 安全管理员	
	□ SQL Server □ Oracle □ Sybase ASE □ DB2 □ 其他	□ 数据库管理系统的鉴别信息有加密和传输保密措施 □ 敏感的系统管理数据加密 □ 敏感的用户数据加密 □ 其他		
	主要应用系统	安全数据保密性	□ 网络管理员	

	□ OA 系统 □ 财务系统 □ 审计系统 □ 邮件系统 □ 其他	□ 主要应用系统的鉴别信息、敏感的系统管理数据加密 □ 主要应用系统的用户数据加密 □ 敏感信息和重要用户信息存储加密 □ 使用便携式和移动式设备时，进行了加密 □ 采用可移动磁盘存储敏感信息 □ 其他	□ 系统管理员 □ 数据库管理员 □ 安全管理员	
数据备份与恢复	网络设备 □ 防火墙 □ 路由器 □ 交换机 □ UPS □ VPN 设备 □ 其他	网络数据备份与恢复 □ 本地数据备份与恢复功能 □ 每天完全数据备份一次 □ 备份介质场外存放 □ 利用通信网络将关键数据定时批量传送的异地数据备份功能 □ 存在关键节点的单点故障 □ 关键网络设备、通信线路和数据处理系统具有高可用性	□ 网络管理员 □ 系统管理员 □ 数据库管理员 □ 安全管理员	

续表

访谈类型	设 备 型 号	访 谈 内 容	访谈对象	备注
数据备份与恢复	操作系统版本 □ Windows 2000/XP/VISTA □ UNIX □ Linux Red Hat/红旗 Linux □ 其他（请注明）	系统数据备份与恢复 □ 操作系统提供本地数据备份与恢复功能 □ 每天一次完全数据备份 □ 备份介质场外存放 □ 其他	□ 网络管理员 □ 系统管理员 □ 数据库管理员 □ 安全管理员	
数据备份与恢复	数据库版本 □ SQL Server □ Oracle □ Sybase ASE □ DB2 □ 其他	数据库数据备份与恢复 □ 数据库管理系统提供本地数据备份与恢复功能 □ 每天一次完全数据备份 □ 备份介质场外存放 □ 其他	□ 网络管理员 □ 系统管理员 □ 数据库管理员 □ 安全管理员	
	主要应用系统 □ OA 系统 □ AO 系统 □ 审计系统 □ 其他	应用系统数据备份与恢复 □ 应用系统提供本地数据备份与恢复功能 □ 每天一次完全数据备份 □ 备份介质场外存放 □ 其他	□ 网络管理员 □ 系统管理员 □ 数据库管理员 □ 安全管理员	
被测评机构下属部门		部门主管姓名		访谈日期
测评机构下属部门		测评人员姓名		

3.2.2　数据安全现场检查

数据安全现场检查过程主要由测评工程师对被测系统的相关文档资料进行比对；对各种与数据安全相关的软、硬件设备进行现场检查（抽查），确认访谈记录与现场检查

的“符合性”。

现场检查与访谈调研的最大区别在于，现场检查要求被测系统的管理或技术人员提供相关的文档、资料或记录等文件以供检查，同时测评人员往往需要对各类设备进行“动手检查”（hands on checking）。动手检查对测评人员而言是一个基本技术要求。作一个形象的比喻，测评人员动手检查的技术水平就好比花样滑冰运动员比赛的时候所进行的“规定动作“比赛。因此要求测评人员对常用的检查手段、环节等非常熟悉。

1．数据完整性检查

在第 3 级安全测评要求中，数据完整性检查一共有如下 3 项。

（1）检查主机操作系统、网络设备操作系统、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否检测/验证到系统管理数据（如 Windows 域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏，是否检测到系统管理数据、身份鉴别信息和用户数据（如防火墙的访问控制规则）在存储过程中完整性受到破坏，以及是否能检测到重要程序的完整性受到破坏。在检测到完整性错误时是否有采取必要的恢复措施的描述；如果有相关信息，查看其配置是否正确。



在检查上述文档或相关证明性材料的时候，应重点查看该项目当初的招投标文件、设计方案和设备技术指标、项目建设过程中的监理文档、建成后的验收材料等。对用于数据安全的专用设备（如数字证书、安全审计软件、杀毒软件和存储设备等），可以在国家有关权威网站上查阅有关型号是否通过了国家权威机构的认证或检验。目前，中国承担各种安全产品认证/检验的权威机构包括（但非全部）中国信息安全产品测评中心、公安部计算机病毒防治产品检验中心、国家保密技术研究所等，本书 1.4 节已经介绍了相关网站，可供有兴趣的读者参考。

（2）检查主要应用系统，查看其是否配备检测/验证系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏的功能；是否配备检测/验证系统管理数据、身份鉴别信息和用户数据在存储过程中完整性受到破坏的功能；是否配备检测/验证重要程序完整性受到破坏的功能；在检测/验证到完整性错误时是否能采取必要的恢复措施。

这一个现场检查项目要求测评人员进行“动手检查”。一个训练有素的工程师应该根据上面的检查要求，按部就班地开展检查。下面模拟一个对“杜甫”子系统中一台业务应用终端计算机的数据安全进行现场检查的情景，供读者参考。在下面各个检查环节中，最重要的是“检查方案”的设计。国家有关标准仅仅是提出测评要求，即测评应该达到的指标，但如何实现则需要测评人员充分发挥艺术想象力，通过设计各种方案来检验被测评对象是否满足这些指标。

检查目标：检查主要应用系统是否配备检测/验证重要程序完整性受到破坏的功能。

检查对象：“杜甫”子系统中某业务应用终端计算机。

检查环境：“天网”工程中心机房。

检查方案：

技术路线

测评人员可以运用多种手段来进行检查，但检查的粒度各有千秋，如可以通过（如果是 Windows 操作系统的话）检查“任务管理器－进程”来查看检查各种正在运行的程序。

然而如何体现“程序完整性”受到破坏呢？这可能需要一个“记录仪”来帮助我们进行检查。因此我们希望能找到一个类似于飞机“黑匣子”一样能够自动记录各种程序活动的小软件。

接下来，就可以设计各种加载/卸载某些应用程序的操作，并使用这个“记录仪”检查这些操作痕迹，从而验证被测设备是否达到标准中所提出的指标。

检查步骤

① 在网上下载辅助工具 RegSnap，并将其安装到待检主机中。

② 单击“启动向导”程序，其界面如图 3.2 所示。



图 3.2　启动向导界面

③ 使用该工具对待测主机新建一个“快照”（单击“新建快照”按钮），以作为系统中应用程序改变之后的对比。此时保存系统快照表在自定义的位置，如图 3.3 所示。



图 3.3　保存快照

④ 现在添加一个应用程序“Dr.Com 宽带认证客户端”，验证是否能够检测到系统完整性受到破坏。

⑤ 添加应用程序后又进行一次快照并保存。

⑥ 选择“比较快照”，观察是否监控到数据完整性受到影响，其结果分别如图 3.4、图 3.5 和图 3.6 所示。

⑦ 为了更进一步验证能否检测到对应用系统文件的恶意删除，卸载“Dr.Com 宽带认证客户端”，立即新建一个快照，随后与刚建的 Dr.Com 宽带认证客户端应用软件的系统进行比较，其结果如图 3.7 和图 3.8 所示。

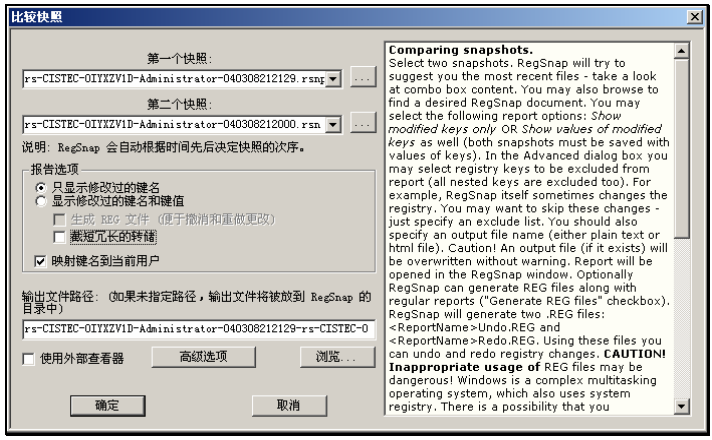


图 3.4　比较快照

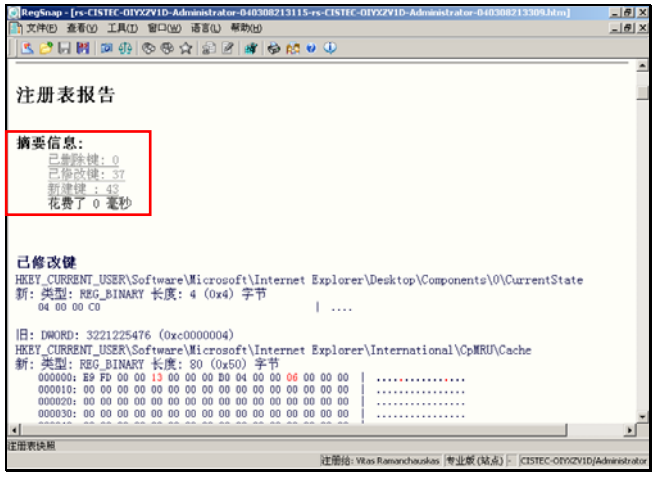


图 3.5　注册表快照（1）

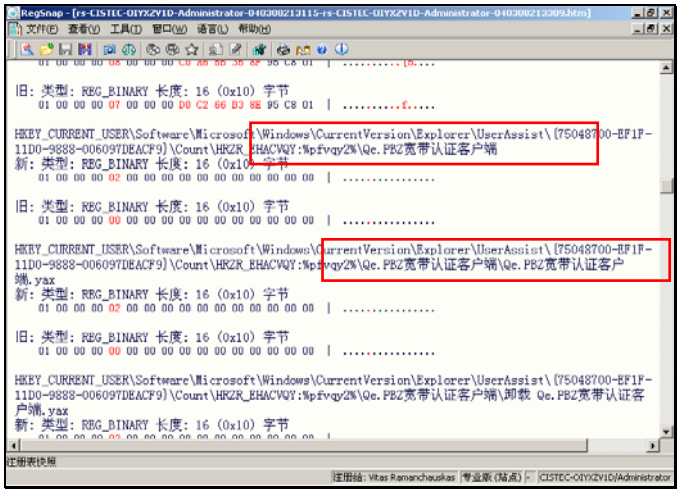


图 3.6　注册表快照（2）

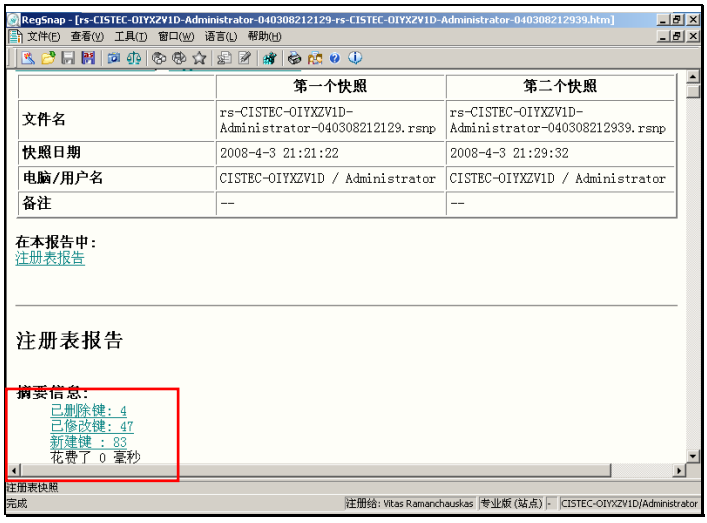


图 3.7　注册表快照（3）

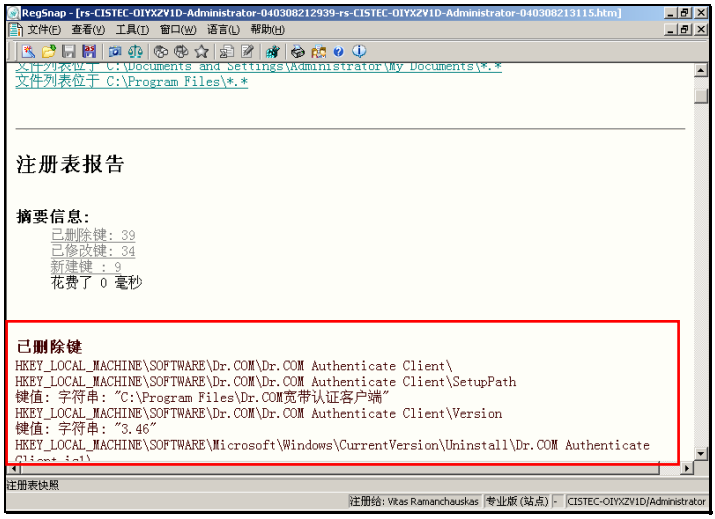


图 3.8　注册表快照（4）

检查结论：“杜甫”子系统中这台业务应用终端符合数据完整性第 3 级保护的有关要求。

在上面这个现场检查的案例中，通过使用 RegSnap 这款辅助软件工具并采用加载/卸载 Dr.Com 宽带认证客户端应用软件等一系列操作来“检测/验证重要程序完整性受到破坏的功能”这个检查要求。因此，一旦发生恶意软件或人员加载恶意程序或卸载重要程序的情况，就能够及时发现。当然，对于更加智能化的恶意软件，有时会通过停止某些重要程序（如杀毒软件的监控程序等）来进行破坏，上述 RegSnap 的功能就显得力不从心了。有条件的读者可以尝试使用主机安全审计系统等方法来加强对重要程序的保护。总之，对同一个安全检查要求，可以达到检查目标的技术路线是多种多样的，它既

取决于所拥有的检查条件，更依赖于测评工程师的想象力。

现场检查的整个过程是通过所谓的检查记录表或类似的文档来体现的，是“安全检查质量保障”的一个必要环节（参见本书最后一章）。下面给出一个模板，谨供读者参考，见表 3.2。

表 3.2　现场检查记录表模板

检查目标	按照国家有关标准，描述相应的检查要求
检查对象	描述待检的设备、型号和版本等，或待检的文档名称
检查环境	设备所处的网络环境及该设备的作用和角色等
检查方案	描述此次检查的主要思路及相关检查工具的说明等
检查步骤	在检查设备的时候，要详细描述检查环节的每一个步骤和动作，并记录每一步所出现的结果
检查结论	对此项检查做出是否符合国家标准相应检查项的结论
人员/时间	检查人员（签章）　　年　月　日

在上面所述的模拟现场检查中，为了使读者能够更好地理解现场检查相关的技术，使用了一个辅助工具 RegSnap。作者在这里需要特别声明的是，我们丝毫没有利用本书推广任何软、硬件产品的打算（事实上，如果要让我们来测试“RegSnap”有些什么缺点，我们也会找出不少理由）。本书选择各种工具的前提条件就是读者可以方便地从网上获得这些免费软件，以便自己进行练习。在实际工作中，读者应该根据本身所承担工作的要求来筛选所使用的各种软、硬件设备，同时要注意这些软、硬件设备是否符合国家有关部门的使用规定。



RegSnap 是一款注册表监视工具。注册表是许多 Windows 家族的核心数据库，表中存放着各种参数，直接控制着 Windows 的启动、硬件驱动程序的装载以及一些 Windows 应用程序正常的运行。而应用软件在安装时，有可能在注册表中注册，将一些必要的信息放进去，如安装时间、使用次数等。RegSnap 就是一种监视注册表变化的工具，以了解应用程序在注册表何处进行了修改。其他类似的工具还包括 RegShot 和 RegMon 等。

在第 3 级安全测试要求中，数据完整性检查的最后一项工作是对“毁伤数据/程序”进行恢复性检查。

（3）应检查主要应用系统，查看其是否配备检测程序完整性受到破坏的功能，并在检测到完整性错误时采取必要的恢复措施。

我们将这个检查工作的具体实现方法留作习题，有兴趣的读者可以自己去尝试。

2．数据保密性检查

在第 3 级安全测评要求中，数据保密性现场检查一共有两项。

（1）检查主要主机操作系统、网络设备操作系统、数据库管理系统、应用系统的设计/验收文档或相关证明性材料（如证书等），查看其是否有关于鉴别信息、敏感系统管

理数据和敏感用户数据采用加密或其他有效措施实现传输保密性的描述，是否有采用加密或其他保护措施实现存储保密性的描述。



第二次世界大战期间，同盟国与轴心国之间的情报侦查与反间谍斗争留下了不少脍炙人口的传奇。当时在葡属印度群岛的一个港口内，隐藏的德军间谍源源不断地向纳粹海军潜艇发送盟军运输船队的信息，致使盟军遭受重大损失。盟军反间谍机关捕获了德军一名情报人员。尽管盟军猜测这名间谍使用了一本海明威的小说作为密码编写脚本，可是却不知道这个脚本隐藏在这本厚厚小说中的哪一页。这时，一名聪明的反间谍人员把小说合拢之后，又慢慢平放在书桌上，于是德军间谍最常用的那一页自然就裂开了……可惜后来英国电影《海狼》忘记了将这个精彩场面编写进去。

该项检查工作主要是各类文档的检查核对。例如，在模拟案例“天网”工程中，就应重点检查巴山市政府信息中心是否提供了以下文档资料：信息系统承建商的资质是否符合相关要求；用于电子政务工作中的终端、操作系统、数据库等在采购环节是否符合国家的有关规定，核心系统是否采用国产设备或通过了国家有关机构的测评（需出具测评报告）；应用软件开发商是否集成了第三方软件，该软件是否符合国家有关数据保密的要求；用于电子公文流转的数字证书是否取得了国家权威机构的认证/检验；用于数据传输的加密设备或网络协议（如 SSL 和 VPN 等）是否符合国家有关标准等。

数据保密性检查的第二项是“动手检查”。

（2）应检查主要应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性。

与数据完整性检查一样，下面给出该项动手检查的模拟过程，以便让读者进一步熟悉现场检查的各个环节。

检查目标：检查主要应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性。

检查对象：“杜甫”子系统中社保资金财务软件应用终端。

检查环境：该终端操作系统为 Windows 2003，配置了 IPsec 模块进行数据保密传输。

检查方案：

技术路线

这项检查要求的核心是“加密或其他有效措施实现传输保密性”。如果仔细研读的话，可知其需要同时满足两个条件，一是加密，二是保密传输。所以可以选择的方案也很多，如先加密，然后再把加密包传出去。目前 Windows/Linux 等主流操作系统本身就带有这个功能，甚至可以直接选择 IPsec 传输模式。所以检查的重点就是查看这台终端是否具有 IPsec 的传输模式并进行加密验证，即通过手工检查，查看是否采用了 IPsec

加密协议及其使用效果。为此，首先检查该终端是否启用了 IP 安全策略，然后人为地加密一个文件来进行验证。

检查步骤

① 检查该终端“安全设置”模块中是否启用了 IP 安全策略，读者可以看到在“安全设置”→“IP 安全策略”这一栏中，该终端对所有 IP 通信均要求使用以古希腊神话传说中的“三头狗”Kerberos 来命名的安全协议（关于 Kerberos 安全协议的介绍不属于本书范围，但读者可以在网上很容易地查询到这个由 MIT 研制的著名安全协议的介绍），其结果如图 3.9 所示。



图 3.9　本地安全设置

② 然后进行文件加密检查。在被测终端的应用系统中任选一个文件夹，本实验以在应用系统中选择名字为“软件”的文件夹为例。单击鼠标右键，选择“属性”→“高级”，再选择“加密内容以便保护数据”，其检查结果如图 3.10 所示。

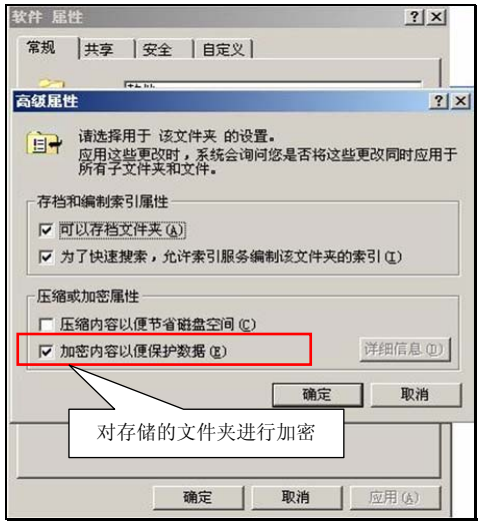


图 3.10　文件加密

③ 然后查看经过加密后的文件夹，可以看到在 Windows 2003 系统中为了区别加密的文件夹，文件变成了绿色，如图 3.11 所示中的标示处。

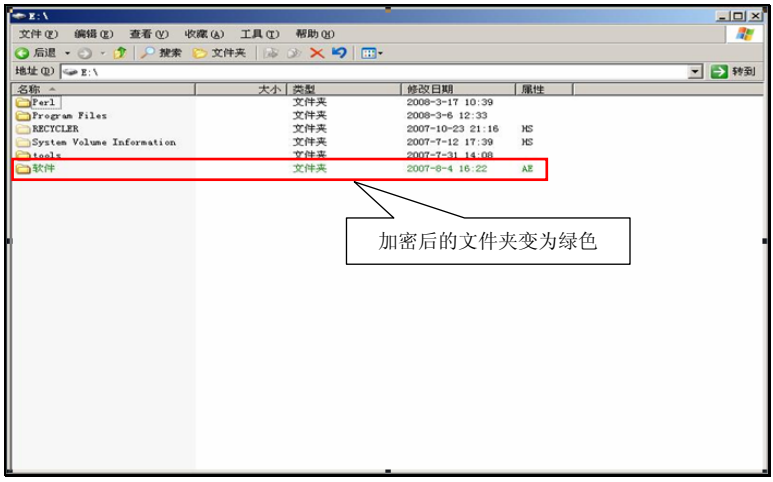


图 3.11　查看加密后的文件夹

检查结论：该终端数据保密性检查符合国家标准的相关要求。

与数据完整性检查相同，在实施数据保密性检查的时候，应该填写《检查记录表》。



最后，针对这个检查案例中所涉及的安全模块，需要提醒读者注意的是，IPsec 模式中所选择的 Kerberos 是 MIT 开发的，其 Version 4 主要用于商业领域，而更高的版本则受美国商务部出口管制。而且它所采用的对称加密算法如 DES、3DES、IDEA 和 AES 等主要是由国外政府机构组织研制，并用于个人或普通商业用途的加密算法（有兴趣的读者可以阅读相关的教材），如果您将来检查的对象有特殊要求，请读者按照国家有关规定执行，如采用国产 SSF33 和 SCB2 对称商用密码的算法等。

3．数据备份与恢复检查

在第 3 级安全测评要求中，数据备份与恢复检查一共有 4 项。

（1）检查设计/验收文档，查看其是否是有关于主要主机操作系统、网络设备操作系统、数据库管理系统、应用系统配置有本地和异地数据备份和恢复功能及策略的描述。

该项检查工作与前面的文档资料检查工作类似，只不过重点要放在数据备份策略等有关文档的检查上，要关注备份与恢复策略的务实性、可操作性。例如，可查看被测单位是否制定了灾难恢复的优先序和应急响应人员“通报树/呼叫树”等（即发生安全事故后的通报流程，请参见本书第 11 章“应急响应”有关内容）。

（2）检查主要主机操作系统、网络设备操作系统、数据库管理系统、应用系统，查看其是否配置有本地/异地备份和恢复的功能，其配置是否正确。

下面以“天网”工程的“杜甫”子系统为例介绍该项检查工作的过程。

检查目标：检查主要主机操作系统，查看其是否配置有本地/异地备份和恢复的功能。

检查对象：“杜甫”子系统数据库服务器。

检查环境：“天网”工程中心机房。数据库服务器操作系统为 Windows 2003。

检查方案：

技术路线

这个检查要求非常明确，就是现场检查操作系统是否配置有灾难恢复与备份（简称“灾备”）功能（注意，不是检查其灾备制度是否完善）。由于条件所限，我们只检查本地灾备功能。具体方法是进入到该数据库服务器操作系统备份与还原向导中进行检查。在该案例中设计了两个结果，一个是没有进行相关备份功能的配置，所以不符合检查要求；另一个是立即进行备份功能配置，从而可以实现对数据进行的备份与恢复功能。由此可见，对现有设备是否进行了合理配置并发挥其功能是进行安全检查工作时的重点之一。

检查步骤

① 用鼠标单击“Windows 操作系统”的“开始”→“运行”，然后输入“ntbackup”命令，进入备份还原向导模块，如图 3.12 所示。

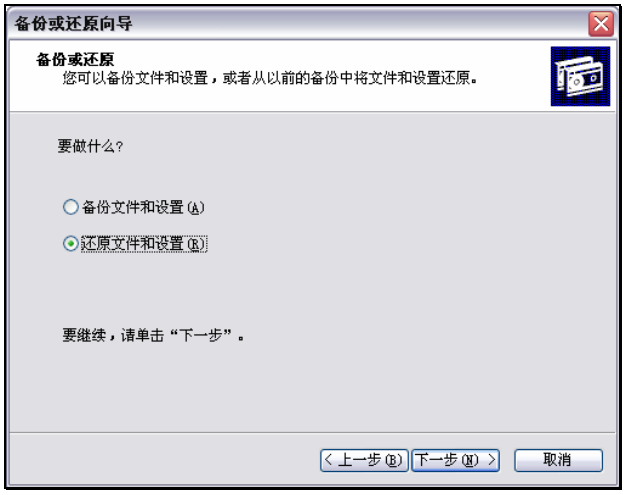


图 3.12　“备份或还原向导”界面

② 选择“还原文件和设置”，查看是否配置了备份功能，如图 3.13 所示。

③ 由于系统没有设置备份功能，所以未能找到数据文件。相反，当用户对主机操作系统设置了备份功能后（见第 1 步，单击“备份文件和设置”），就能够找到数据文件，如图 3.14 所示。

④ 下一步就可以完成还原，如图 3.15 所示。

检查结论：该数据库服务器具有本机数据恢复功能，经正确设置后能满足数据本机恢复的要求。

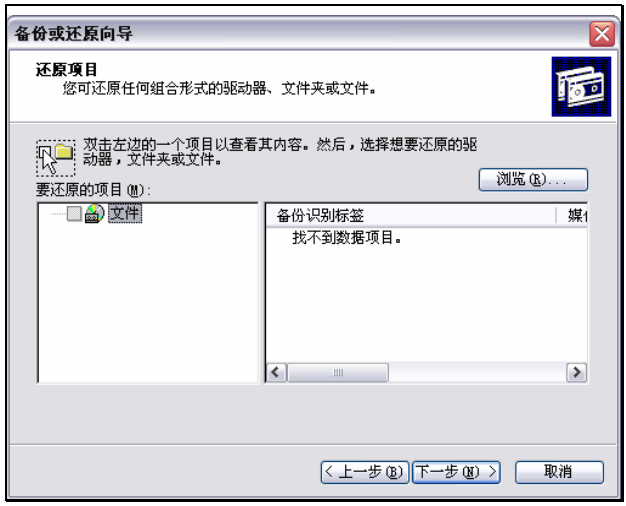


图 3.13　还原功能设置（1）

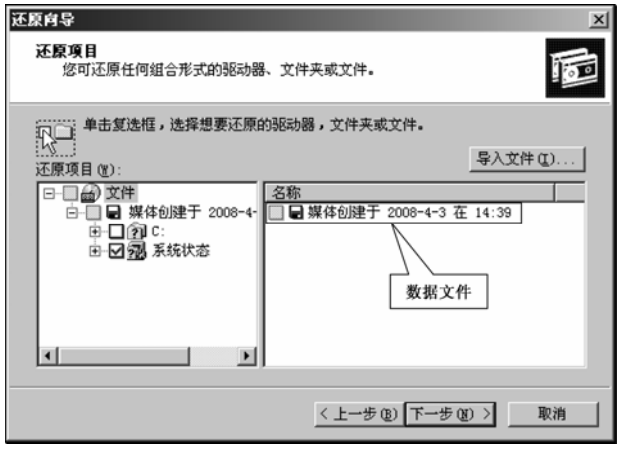


图 3.14　还原功能设置（2）



图 3.15　“完成还原向导”界面

（3）检查主要网络设备、通信线路和数据处理系统是否采用硬件冗余、软件配置等技术手段提供系统的高可用性。

该项检查也属于“动手检查”，但工作方式与上面有所不同。测试人员这时应该对被检网络进行实地考察，并绘制相应的网络拓扑图。当然，这些信息也可通过检查被测单位提供的相关文档资料来获得。

检查目标：检查主要网络设备、通信线路和数据处理系统是否采用硬件冗余、软件配置等技术手段提供系统的高可用性（健壮性/鲁棒性）。

检查对象：“天网”工程系统基础网络

检查环境：“天网”工程主机房

检查方案：

技术路线

“天网”工程系统的高可用性是进行数据备份与恢复的前提条件。而系统的高可用性和系统健壮性/鲁棒性则是一个非常宽泛的概念。为了说明一个系统具有高可用性，需要检查验证的项目有很多。但总体上来讲可以分为系统容错能力、系统负载均衡能力、备份设备、磁盘备份分区等一些必备的检查项目。

在“天网”工程大型网络环境中，整体系统架构是否具有高可用性，可以从系统的基础结构来检查，如是否有安全的防火墙保护；是否有冗余的域控制和 DNS；是否有网络负载均衡和冗余虚拟服务器；是否有服务器群集、存储组配置和 Exchange 数据分区、RAID 配置、SAN 或 NAS 技术；是否有高性能备份设备；是否有监视服务器等方式，等等。

检查步骤

① 系统容错。检查是否有安全的防火墙保护；是否有冗余的域控制和 DNS；是否有网络负载均衡和冗余虚拟服务器；是否有服务器群集、存储组配置和 Exchange 数据分区、RAID 配置、SAN 或 NAS 技术；是否有高性能备份设备；是否有监视服务器。图 3.16 是模拟检查“天网”工程系统容错性的时候所发现的相关容错设备。

② 负载均衡。查看是否具有网络负载平衡功能的前后端体系结构。我们设计的案例是对 Exchange 2003 前后端服务器集群进行网络负载均衡的检查（其中负载均衡共享地址为 10.0.0.2），检查后绘制的草图如图 3.17 所示。

③ 检查服务器集群，发现其中包含了备用节点。检测后的草图如图 3.18 所示。

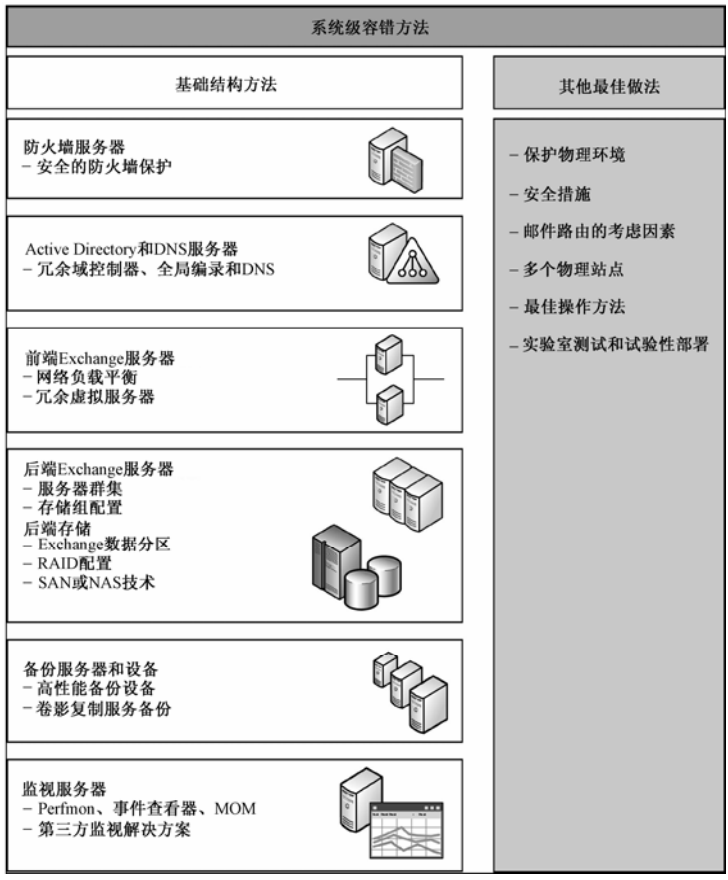


图 3.16　系统级容错设备检查图

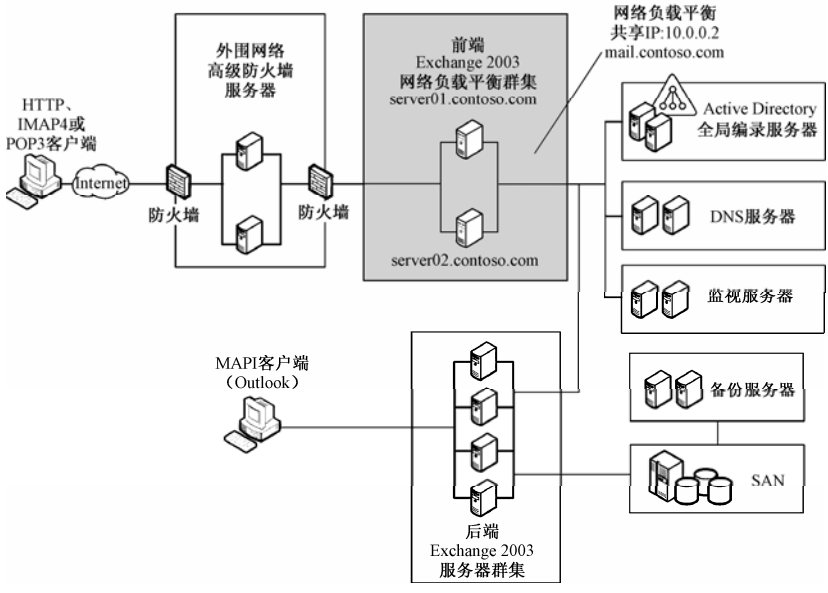


图 3.17　负载均衡检查

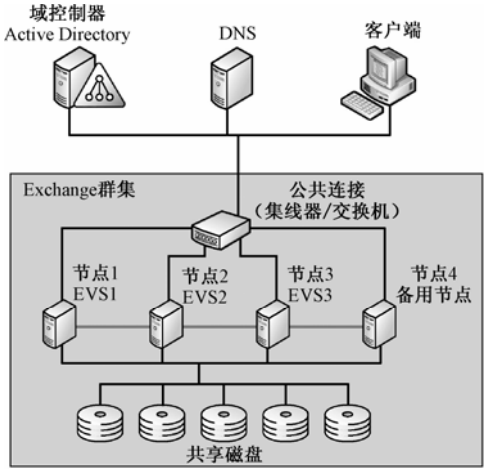


图 3.18　备用节点检查

④ 对 Exchange 硬盘的分区和容错硬盘设置进行检查，其结果见表 3.3。

表 3.3　硬盘分区检查表

磁盘	驱动器配置
硬盘 1	驱动器 C（NTFS）—— Windows 操作系统文件和交换文件
硬盘 2	驱动器 D（NTFS）—— Exchange 文件和其他服务器应用程序（例如，防病毒软件和资源工具包）
硬盘 3	驱动器 E（NTFS）—— 存储组 1 的事务日志文件
硬盘 4	驱动器 F（NTFS）—— 存储组 1 的数据库文件
硬盘 5	驱动器 G（NTFS）—— 存储组 2 的事务日志文件
硬盘 6	驱动器 H（NTFS）—— 存储组 2 的数据库文件

检查结论：符合国家标准对该检查项的要求。

（4）检查网络拓扑结构是否不存在关键节点的单点故障。

所谓关键节点的单点故障，通俗地讲就是“瓶颈”。一旦该点出现故障（人为操作失误、黑客攻击或设备老化等）就将导致整个网络运行效率降低甚至中断。因此应当检查网络拓扑结构中，当子系统内某种设备出现故障或受到攻击后，某个子系统或其他子系统能否正常工作，查看拓扑图上是否有重要系统的备份设备（是否有采取转移或恢复措施），等等。关于此项的检查工作留作习题请读者思考。

3.2.3　数据安全测试

现在进入测试环节。如果说本书上面介绍的现场检查工作是花样滑冰运动员的“规定动作”表演，那么测试工作就是测试工程师的“自选动作”表演了。

数据保密性测试：在第 3 级安全测评要求中，测试项只有一项，即对数据保密性进行（无损渗透）测试，对“数据完整性”和“数据备份与恢复”没有测试要求。

该项测试应测试主要应用系统，查看其是否采用了加密或其他有效措施实现传输的

保密性。

正如本书前面所描述的那样，在指导测评工作的时候，任何一个国家标准都只能提出“原则性、普适性”的测评要求和目标，而如何实现这个目标，国家标准不会也不可能给出具体的操作步骤。而恰恰在这个时候是一名工程师充分发挥其测评艺术想象力的机会。下面就按照“5W+H”（参见本书第 2 章）的思路，来组织这个测试。

测试目标：数据保密性测试。检验信息在传输过程中是否采用了加密或其他防范措施。

测试对象：“杜甫”子系统中处理巴山市政府内部电子公文的应用终端系统。该终端系统虽然属于“天网”工程系统的 G2P 子系统（即外网），但由于该终端系统定位为处理政府内部公文，如存储、传输和处理国家社会劳动保障与人事部的有关公文、巴山市政府社会劳动保障局的政府公文等，所以一般情况下应该与“杜甫”子系统的其他业务终端相隔离（物理隔离或高强度逻辑隔离），以保证该机能够接入“天网”的 G2G 内网。

测试环境：“天网”工程中心机房。

测试方案：

技术路线

该项测试要求与前面进行的数据保密性现场检查的第（2）项要求有所不同。在数据保密性现场检查中，仅仅检查了被检终端是否使用了安全通信模块（如上面的案例中使用的 Kerberos 协议模块），是否能够进行文件加密处理，等等。而在这里，需要“亲眼所见”信息在传输过程中是否采用了加密或其他安全保密措施。所以，需要在网络协议层进行数据包的截获和分析，以查看是否进行了加密处理。为此，就需要使用协议分析工具。

具有协议分析功能的工具既可以是硬件设备，也可以是软件工具。为便于本书读者动手练习，我们选择了人们能够从网上自由下载的软件工具。

测试环境的搭建是需要考虑的另外一个问题。由于是模拟测试，所以在本书中仅仅是在被测试的主机上运行一款协议分析工具，并连接另一台主机使之与其进行通信。

接下来将利用这款协议分析工具捕获该主机传输的数据包并对其数据包的有效载荷部分进行分析，检查是否进行了加密处理。



Ethereal 是一个带图形用户接口（GUI）的网络嗅探器，能够完成与 tcpdump 相同的功能，但操作界面要友好很多。Ehtereal 和 tcpdump 都依赖于 pcap 库（libpcap），因此两者在许多方面非常相似（如都使用相同的过滤规则和关键字）。其他的网络嗅探器还包括大名鼎鼎的 Sniffer 等。读者千万不要局限于本书工具的选择，而要充分发挥自己的创造性来选择和使用这些工具。

测试步骤

① 在网上下载并安装 Ethereal 软件。

② 对 Ethereal 进行设置。打开 Ethereal 软件的操作界面，对其网卡进行设置，由于本实验是在虚拟机上实现的，所以选择虚拟机网卡接口，如图 3.19 所示。

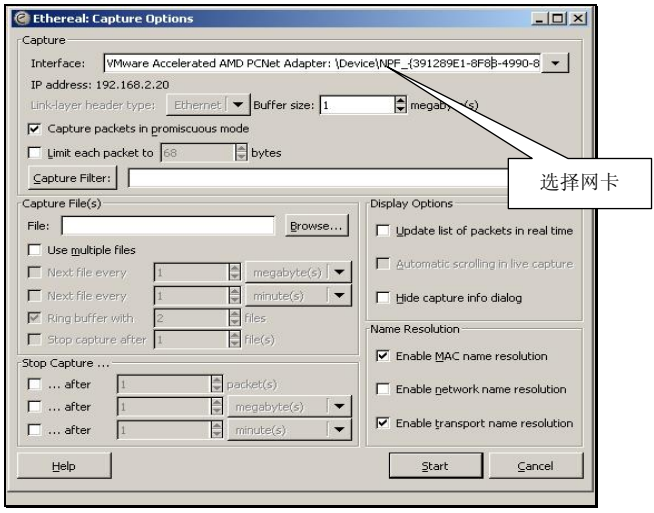


图 3.19　Ethereal 虚拟机网卡接口

③ 捕获通信数据包。单击“start”按钮，以便让 Ethereal 捕获该主机与其他终端的数据包，如图 3.20 所示。

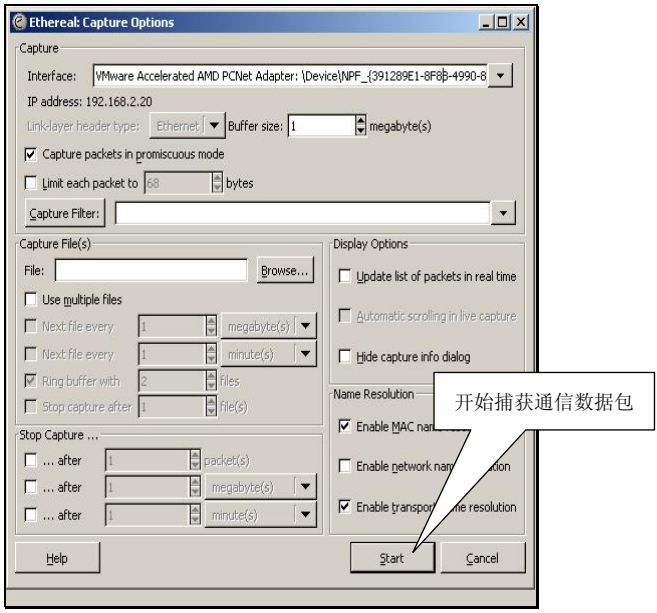


图 3.20　开始捕获数据包

④ 运行一段时间后，停止 Ethereal，并在该工具的界面上查看捕获的数据包。利用 filter 来选择该主机应用系统的通信协议。在实际测评工作中，读者应该根据具体情况来逐一测试所应用的通信协议（在本书中选用的是邮件通信协议 Post Office Protocol，即 POP3。人们在使用 POP3 协议的时候，安全保密性是需要特别关注的焦点）并查看该类协议的数据包是否进行了加密处理。从 Ethereal 所捕获的“乱码”数据包可以看出，POP 通信协议层上的数据包进行了加密处理，如图 3.21 所示。

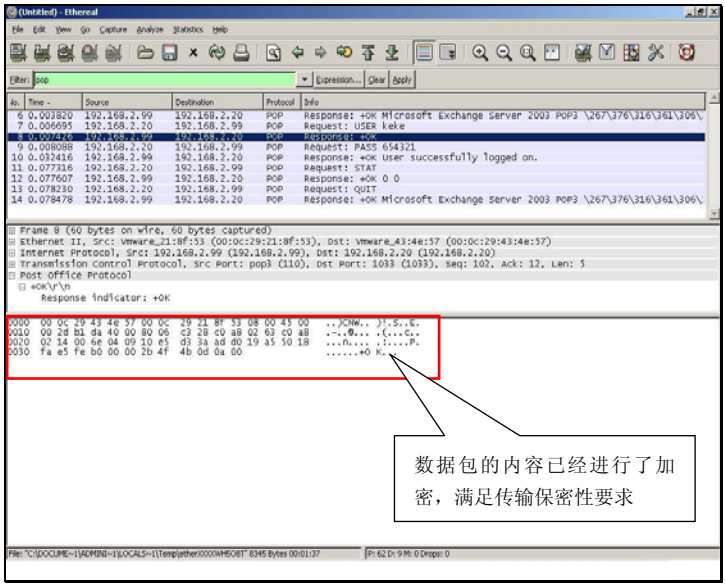


图 3.21　加密处理后的 POP3

⑤ 重复上述步骤以确认实验结果无误。

⑥ 根据需要可再选择其他通信协议并检查所捕获的数据包。

测试分析：经过选择不同的通信协议和反复实验，该测试对象所传输的数据包均进行了加密处理，所以可以有效地防范在传输过程中对数据包的非法拦截、窃听和破译等安全威胁。读者可能会注意到，我们在进行实验分析时的谨慎态度，即仅对数据包的传输过程进行了分析，而数据的存储是否也需进行加密处理，这里并未涉及，对此您可以提出自己的实验方案。另外，需要再次向读者强调关于加密算法的使用要符合国家有关规定的要求，尽管这并不属于本次测试的范围。

测试结果：该测评对象满足数据安全第 3 级安全测评要求。

最后希望提醒读者注意，测试完成之后应该出具数据安全测试技术报告。

数据安全测试技术报告的撰写格式风格各异，但主要内容应当包括上面已经提到的测试目标、测试对象、测试环境、测试方案、测试步骤、测试分析和测试结论，等等。表 3.4 是数据安全测试技术报告的一个模板，仅供读者参考。

表 3.4　数据安全测试技术报告模板

测试编号	为了便于管理和测试案例重用，建议对测试案例进行编号。编号的方式有很多，包括采用“拼音＋数字”的方式。例如，TC-TW-SJAQ-001（“天网数据安全 001 号测试”）。也可严格按照国家有关档案管理的标准进行编号
测试目标	明确此次测评所需达到的要求，即相关标准对该项测评工作的描述
测试对象	描述测试对象的型号、在该信息系统中的作用，等等
测试环境	一般可以使用图例的方式来进行描述，同时还可以使得有关人员在需要的时候能够搭建相同的环境进行实验重现
测试方案	测试方案也称测试技术路线，它反映了一名测试工程师是如何根据测试要求来设计所需要的输入和输出结果的
测试步骤	详细描述测试的各个步骤。一般可将每个步骤所出现的结果（图文）置于此处，以便阅读该报告的人员在需要的时候能够重现结果
测试分析	根据测试过程中的各种输出结果，进行标准“符合性”分析
测试结果	对此次测试实验是否通过下结论
测试人员/时间	测试人员（签章）　　年　　月　　日

至此，就完成了对巴山市政府电子政务“天网”系统中的“杜甫”子系统的数据安全测评。需要提请读者注意的最后一个问题是，测评工作结束后，应当出具一个有关“杜甫”数据安全的整体测评技术报告。该报告由上面所介绍的各个测评子项技术报告、表单等组成。然后对其进行统计分析，如有哪些项满足国家有关标准要求，哪些项不满足或不完全满足国家有关标准要求，等等。统计结果可以用柱状图、饼状图等直观的方式来展现。而这个数据安全测评技术报告最后又将与其他的测评技术报告（如网络安全、主机安全和应用安全等）合并在一起，由测评工程师进行全面分析之后，给出“天网”（第 3 级）信息安全测评总技术报告。由于本书篇幅所限和考虑到本书读者的背景，这里略去这个文档化工作部分。

3.3　本章小结

- 数据安全测评的三种主要方法
- 数据完整性测评
- 数据保密性测评
- 数据备份与灾难恢复测评
- 访谈工作中要注意的问题及其访谈艺术
- 现场调研的问卷调查表
- 现场文档检查的要点
- 现场动手检查的流程与检查报告或记录
- 现场测试的方案设计与测试技术报告或记录

尾声：窃之犹在！

试给出下面两个问题的答案:

第一个问题，假设你总共有 1 万元，被盗走了 1 万元，现在还剩多少？

第二个问题，假设你本来共有 1 万元，现在还有 1 万元，有没有被盗？

如果你回答，第一个问题，0；第二个问题，“没有”。那么，……祝贺你！答对了！

如果你回答，第一个问题，1 万元；第二个问题，……不知道。那么，……恭喜你，又答对了！

请君细细想想。

一般的东西，别人盗走了，你就没有了。但是有一种东西，别人盗走了，你还有，而且是完完全全仍拥有，没有半点残缺。这种东西是什么？

它就是信息！它就是数据！

数据被窃，你的还在，这是好事吗？

不，这恰恰是一个世纪难题之源。为什么？因为你很难发现你的东西被盗，因为它好好地在那儿。打个比方，就好像是你的东西被盗，却没有被盗的结果，无法通过结果“报案”。

如何解决这个难题？目前，除了防范让被盗不发生外，就只有通过“盗窃”的行为痕迹来发现了，而不是被盗的结果。信息加密其实并不是直接从根本上解决信息被盗的问题，而是间接的，即让被盗走的东西“不能用”。

不知不觉就被盗，被盗了还浑然不知。这其实是最可怕的被盗了。有没有法宝来解决这个信息被盗的难题？

有！它叫做量子通信。

简单地说，量子保密通信的根本原理是海森堡测不准原理，量子态的各分量（如位置和动量）不可能同时被精确测量。当量子态作为信息表达时，如果要盗取它，就必然破坏它，因而不仅盗取无用，而且会被立即发现。

2005 年初，由潘建伟、王向斌、杨涛、彭承志和马怀新等人组成的联合研究小组开始利用诱骗信号方法进行远距离量子密钥分发的研究。经过近两年的联合攻关，2006 年夏，他们在国际上率先取得并宣布距离大于 100 km 的实验结果。

2007 年 1 月，由清华大学、中国科技大学等单位组成的联合研究团队于近期在远距离量子通信研究上取得重大突破，在国际上率先实现绝对安全距离大于 100 km 的量子保密通信。

2008 年 3 月 28 日出版的《物理学新杂志》，发布了一项意大利和奥地利科学家的研究成果，他们首次识别出从地球上空 1500km 处的人造卫星上反弹回地球的单批光子，实现了太空绝密传输量子信息的重大突破。这一突破表明在太空和地球之间可以构建安全的量子通道来传输信息，以用于全球通信。

我们期待着一个革命性的量子计算时代的到来。

观感

（1）数据安全包括哪几个方面？

（2）访谈调研中使用问卷调查表的好处是什么？

（3）访谈、检查和测试这三个环节之间的相互关系是什么？

（4）现场检查工作中的动手检查与测试工作的异同何在？

（5）请在网上查阅中国从事有关“数据修复”业务的机构。

（6）请使用 Sentinel 工具，完成数据完整性现场检查。要求是：检查一台终端主机，查看其是否配备检测程序完整性受到破坏的功能；并在检测到完整性错误时能采取必要的恢复措施。

（7）请使用 Sniffer 工具或您认为合适的工具来重复练习本书数据保密性测试，并提交测试报告。测试报告应包括以下内容：实验目的、实验方案、实验环境（平台）要求、实验步骤和实验结果分析等。

（8）“天网”工程系统中面向社会服务的分系统 G2P 有一个子系统，即该市的“劳动与社会保障信息系统”（我们称为“杜甫”子系统，取其“安得广厦千万间”之意）。“杜甫”子系统承担了向全市市民提供劳动与社会保障服务的功能，如就业信息、养老保险发放和医疗保险支付，等等。根据该子系统对全市市民正常工作和生活的重要性，“杜甫”子系统的安全等级被定为 3 级。该子系统的数据中心采用双机容灾集群配置，磁盘采用 RAID 技术提供磁盘镜像，并配备磁带库数据备份系统。当某一通信线路、路由器、防火墙、交换机或服务器出现故障时，相应的备份通信线路，以及冗余的路由器、防火墙、交换机和服务器接管工作。当数据磁盘出现故障时，可以采用 RAID 磁盘镜像以及数据备份系统进行数据恢复。数据中心配置了一台数据库服务器、一台应用服务器、一台磁盘阵列设备、一台备份服务器、两台网络交换机，两台路由器。“杜甫”子系统网络拓扑图如图 3.22 所示。

① 请根据国家标准设计一份“杜甫”子系统数据安全访谈问卷调查表。

② 请了解 RAID 技术在数据备份与恢复工作中的作用。

在此基础上提出您对“杜甫”子系统数据完整性现场检查的工作要点。

（9）“天网”工程部分子系统网络拓扑图如图 3.23 所示。其中办公自动化子系统（OC）、财务子系统（F）、数据汇聚子系统（D）、协同办公系统（G）之间都划分在一个 VLAN 内，这是否会导致“故障连锁反应”？通过拓扑图上 OC 和 F 这两个子系统的服务器有无备份说明该系统是否符合第 3 级安全测评要求中关于关键节点单点故障的检查要求。

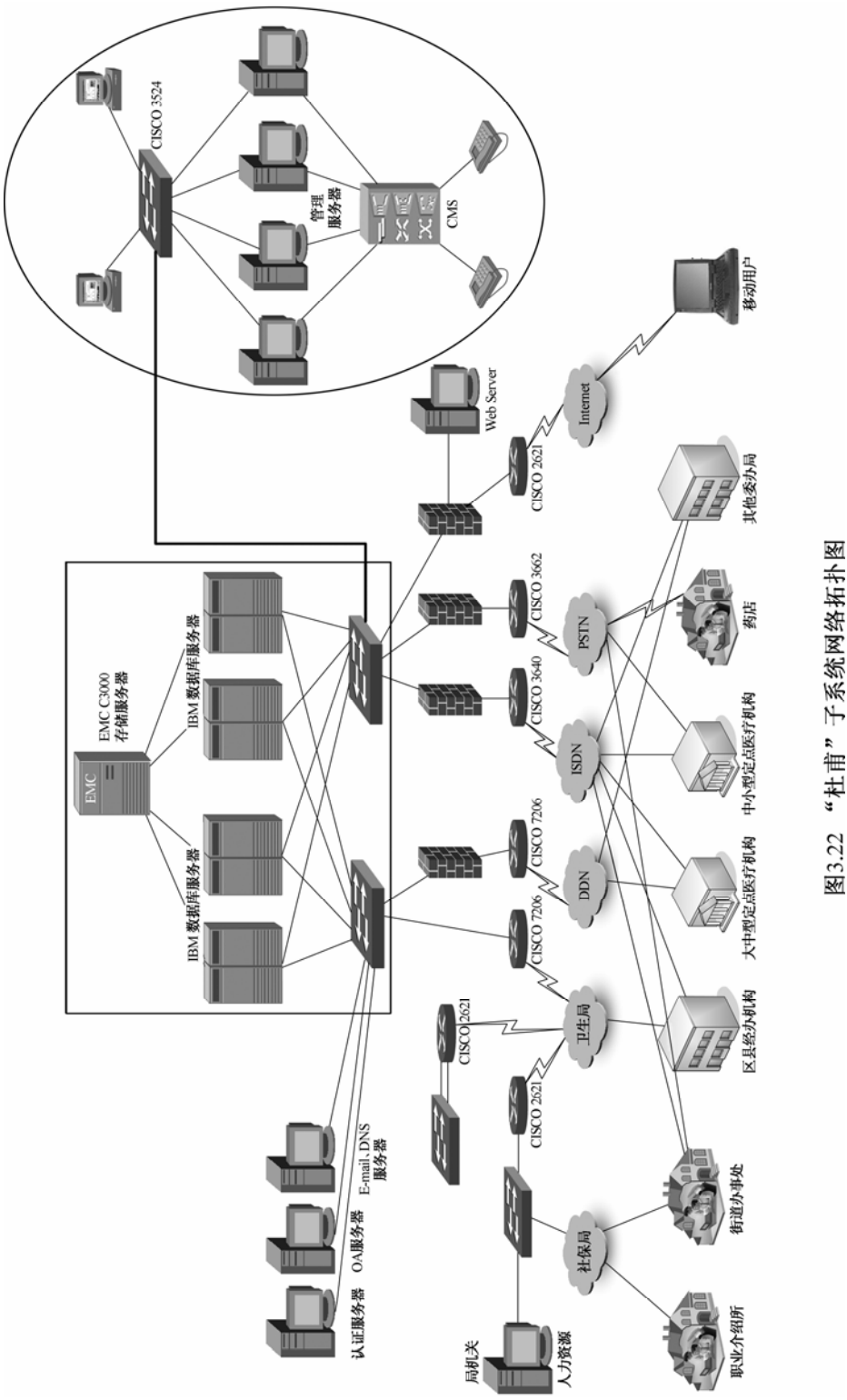


图3.22　“杜甫”子系统网络拓扑图

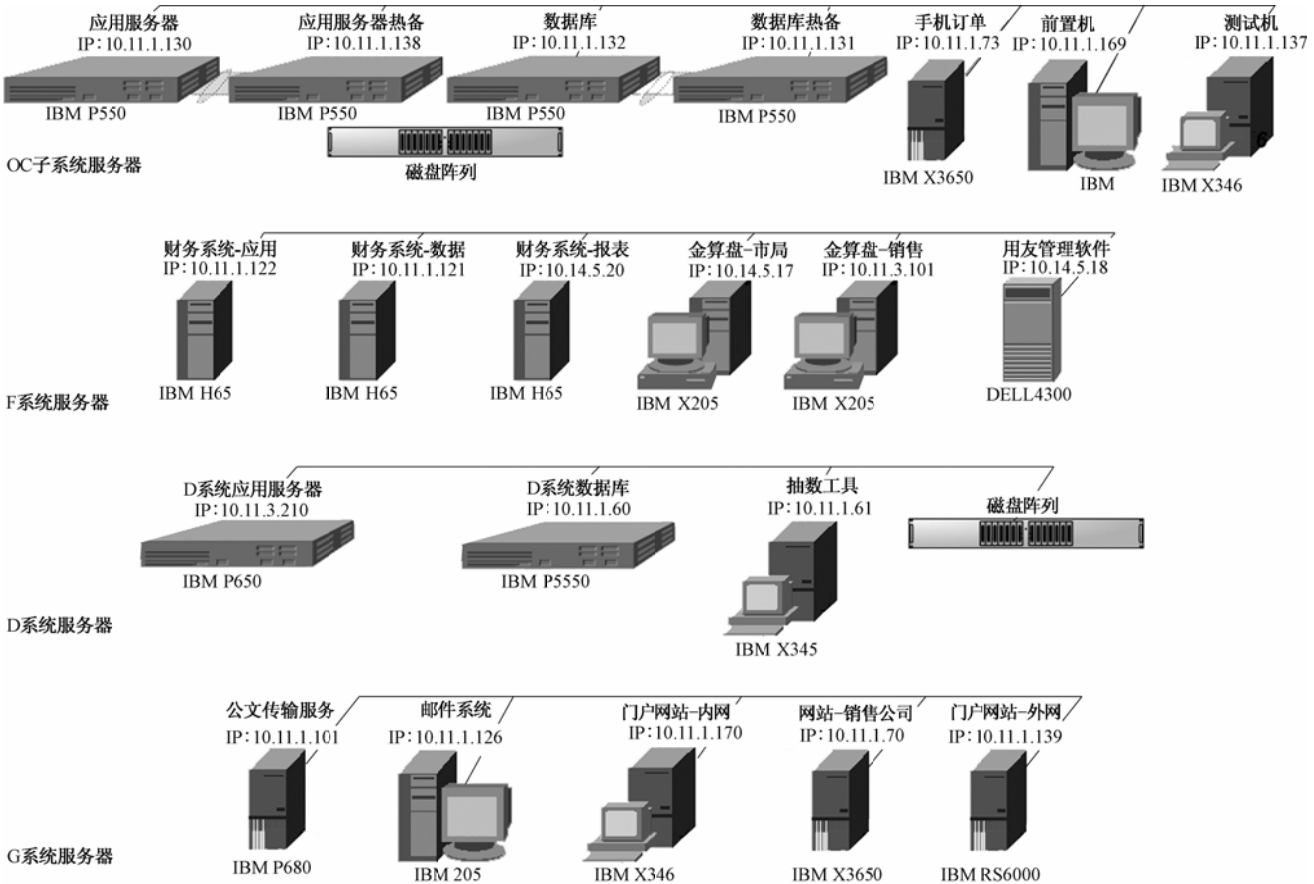
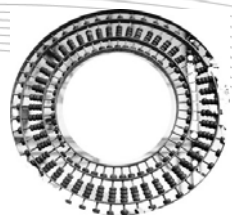


图3.23 “天网”工程部分子系统网络拓扑图

第 4 章
主机安全测评技术





最古老的计算机——算盘

Mens et Manus（既动脑 又动手）

——麻省理工学院校训

序幕：第一代黑客

1861 年，立志于改变当年美国高校迂腐的教育方式和死记硬背的学习方法，为美国的崛起培养新型人才的退休教授 W·B·罗杰斯（William Barton Rogers）以“基础科学与应用科学并重，教学工作与科研活动相结合，学校教育与社会需要相联系”为办学宗旨，四处化缘，创办了一所职业技工学校——麻省理工学院（MIT）。

1961 年，在处处洋溢着百年校庆喜悦氛围的 MIT 校园里，那帮成天琢磨着自己动手拼装工具，眼梢瞟着查尔斯河对岸哈佛大学俊男靓女们的 MIT 学子当中，又在悄悄流传着一个振奋人心的消息：该校著名的林肯实验室推出了世界上第一套“分时计算机系统”（CTSS），从而使得学生们都有希望拥有自己的计算机终端！（想想我们现在的条件有多好！“我的机器我做主!”）接下来这些现代鲁班们沉醉于给“自己的计算机”编写各种应用程序，再加上 MIT 特有的“恶作剧”校园文化，世界上第一代黑客就顺理成章地诞生了……

本章的目的是希望读者始终保持这种“在大海边拾贝”（牛顿语）的好奇心，探索主机安全的测评技术，使您能够成为一名合格的安全测评工程师。至于您是否也梦想着与 MIT 的这些“顽童们”“打擂台”，我们含笑不语。

要点：本章结束之后，读者应当了解和掌握

- 主机安全测评的 8 个环节是什么？
- 主机安全测评的 3 种手段是什么？
- 怎样进行主机安全测评？

4.1 主机安全测评的诸方面

首先，请教读者一个简单的问题：什么是主机？提出这个问题并非是作者有意要挑战您的知识底线或者是不合时宜地要考您“脑筋急转弯”，而是希望您从更深刻的层面



1900 年，伟大的爱因斯坦正在为争取获得伯林大学的博士学位而发愁，美国则正在往德国派遣大量留学生。而中国的慈禧太后却沉醉在让“刀枪不入”的义和团入京护驾的神话之中。那个年代全中国懂得微积分的人不超过 10 人……1967 年，在美国研发出世界上第一台计算机分时系统之后仅仅 6 年，由中国科学院蒋士騵领衔设计、专为“两弹一星”服务的中国第一台具有分时、中断系统和管理程序的计算机——“109 丙机”交付给张爱萍上将领导的国防科委使用。在这台计算机上运算了一代又一代的中国撒手锏战略武器，并一直用到 20 世纪 80 年代，因此被誉为“功勋计算机”。

理解主机安全测评的含义。从系统科学的角度来讲，一个复杂的信息系统就是一个社会组织，是由形形色色的社会成员组成的，他/她/它们分工协作，共同完成人们赋予这个信息系统的各项任务。从某种意义上来讲，“主机安全”是整个系统安全的“最后一道防线”，整个信息系统的安全取决于每个成员的安全。这个社会成员就是各种型号的计算机（包括软、硬件）以及管理和使用计算机的人员。因此，本章题目虽然是“主机安全测评”，实际上您要测评的对象并非仅仅是一台冷冰冰的机器盒子，而是包括使用这台计算机的人在内的“人–机合一”系统。为此，与第 3 章数据安全测评一样，国家标准仍然从管理和技术两个层面，分为“访谈”、“检查”和“测评”三种手段对主机安全测评提出了若干条款。

我们理解性急的读者跃跃欲试、“磨刀霍霍向天网”的心情。但在剖析“天网”工程各个主机的安全之前，至少应了解一下国家标准中有关对主机安全测评的这些条款内容吧？与第 3 章不同，主机安全测评的注意力将不再是“数据完整性”、“数据保密性”和“数据备份与恢复”方面。国家标准中把主机安全测评的数十项条款划分为“身份鉴别”、“自主访问控制”、“强制访问控制”、“安全审计”、“剩余信息保护”、“入侵防范”、“恶意代码防范”和“资源控制”8 个环节。具体的测评方式将在 4.2 节“天网”案例中进行描述。为了避免与其他有关信息安全的教材内容重复，同时也处于节约本书篇幅和增加可读性的考虑，下面仅仅是形象化地介绍相关的基本概念，建议有兴趣的读者可以参考其他介绍主机系统安全的教材，以了解其详细、科学的定义，熟悉这些概念的读者则可以跳过本节。

（1）身份鉴别。您需要出示相关证件才能进入一个企事业单位，这在国内外都是常识。同样地，在登录一台计算机终端或服务器的时候，需要有对登录人员身份进行鉴别的机制。身份鉴别主要包括登录口令和用户名等内容，更高级的鉴别技术则包括数字证书、指纹识别、虹膜识别，等等。

（2）自主访问控制。进入单位大门之后，如果您还要访问重要的部门，那么您还需要佩戴不同级别的识别牌。主机内部也应该有这类访问控制机制，分为**自主访问控制**和**强制访问控制**，它们主要是对登录后的用户进行访问权限的管理。所谓的自主访问控制是指用户可以按自己的意愿对主机的参数做适当修改以决定哪些用户可以访问他/



“捉鬼”与“捉虫”。在计算机测试行业，有一位帅哥和一位靓女的故事可谓异曲同工。Grace Hopper，这位后来美国海军的首席女科学家和海军少将，当初在第一代计算机 Mark I 研发工作中扮演的角色是“捉虫”，她将造成电路短路的一只飞蛾抓了出来，这就是我们今天说的 debug。而被喻为当代毕升的王选，当初北京大学数学系的本科生，在参与研发中国第一代计算机“红旗机”的时候，他的主要职责之一就是拿着一个榔头去轻轻敲打“红旗机”的主板，以发现电路焊接过程中是否有“虚焊”现象。如果一敲，机器停止运算了，就又发现了一个安全隐患，所以他将这个工作称为“捉鬼”。

她的文件。

（3）强制访问控制。所谓强制访问控制是指用户与文件都有一个事先设置的、非经授权不能修改的安全属性。这些属性是强制性的规定，它是由这台主机的安全管理员（而非这台主机的一般用户），或者是操作系统根据限定的规则确定的，用户或用户的程序不能加以修改。主机用该安全属性来决定一个用户是否可以访问某个文件。

（4）安全审计。形象地讲，安全审计就是使“做了坏事跑不掉”。所以主机安全审计包括对主机系统安全日志的保护，对用户行为的记录，以及对主机资源的异常记录等方面。

（5）剩余信息保护。在悲壮的战争影片中，当敌人就要冲进我方指挥所的时候，您会看到什么场面？砸毁电台和烧毁密码本！剩余信息保护就是主机储存“敏感信息”的空间被释放给其他用户的时候，原来储存在主机里面的重要信息（用户的鉴别信息和文件目录等）要保证及时清理掉。

（6）入侵防范。“如果有人在干坏事要及时发现和快速反应”。入侵防范包括对入侵行为的记录（攻击的目的、攻击的时间、攻击者的 IP 地址、重要程序是否被破坏以及破坏之后能否迅速恢复等）。

（7）恶意代码防范。预防天花的有效方法是种牛痘。恶意代码防范主要是检查主机是否配备相关的防恶意代码的机制，包括杀毒软件，等等。要注意恶意代码的定义已远远不是大家常说的“恶意病毒”，还包括木马、“间谍软件”等恶意程序。

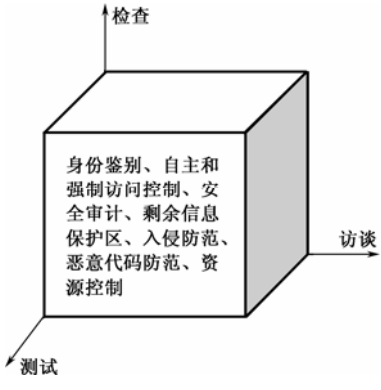


图 4.1　主机安全测评的框架图

（8）资源控制。可以把它理解为现代环保主义思想在主机上的典型体现。用户不能无限制地使用主机资源，也要防止外面的用户非法掠夺这台主机的资源。

对主机安全进行测评，实际上就是对上述八个方面，利用访谈、检查和测评等手段进行分析。主机安全测评的框架图如图 4.1 所示。

4.2　主机安全测评的实施

假设根据“深海”信息安全测评中心制定的工作计划，现在进入了对“天网”工程系统的主机安全测评阶段。假设此次的测评对象（主机）属于“天网”的 G2G 政府内部办公网络“青天”子系统。“青天”子系统用于巴山市政府的内部办公业务，其服务对象主要是政府各部门的公务员（与“杜甫”子系统的服务对象不同），他们处理的各种政府公文很多带有敏感性，如尚未出台的各种政策文件，正处于调查取证阶段的各种职务犯罪案件的电子文档等。根据事先的等级评定，将“青天”子系统安全等级也定为 3 级。顺便指出，即使“青天”和“杜甫”在安全等级上均属于第 3 级，但这并不意味着这两个子系统可以完全不设防地互联互通。仍然需要使用安全域等概念对他们之间的信息共享机制加以约束。

现在需要根据国家制定的关于主机第 3 级安全测评要求进行工作。

4.2.1　主机安全访谈调研

主机安全访谈调研过程主要是由测评工程师与被测评单位的各级系统管理人员、安全检查员、安全审计员、各个主机的使用者等进行的问卷式访谈。首先介绍第 3 级安全测评要求的访谈内容，然后与第 3 章一样，通过一个访谈问卷调查表模板来细化这些访谈内容。国家标准关于第 3 级主机安全访谈共有 5 类 9 项，分别如下所述。

1．主机身份鉴别访谈

第 3 级安全测评要求主机身份鉴别访谈共有 3 项：

（1）应访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现。

（2）应访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现。

（3）应访谈主要操作系统和数据库管理员是否采用了远程管理，如采用了远程管理，查看采用何种措施防止鉴别信息在网络传输过程中被窃听。

2．主机安全审计访谈

第 3 级安全测评要求主机安全审计访谈只有 1 项：

应访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统对事件进行审计的选择要求和策略是什么？对审计日志的处理方式有哪些？

3．主机剩余信息保护访谈

第 3 级安全测评要求主机剩余信息保护访谈共有 2 项。

（1）应访谈系统管理员，询问操作系统用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除。



“僵尸网络”（BotNet）是目前发展非常迅速的一种安全威胁。据联合国统计，全球在2007 年共有数百万台计算机终端沦为“僵尸”，一旦被驱动发作，将成为威力极大的“信息定时炸弹”。因此对“僵尸网络”的防范是目前研究的热点问题之一。从另外一个角度来讲，如果将互联网比喻为一个巨人，计算机终端就如同人体身上的细胞。我们是否需要对每一个细胞的健康状态加以关注呢？这样做需要花费什么样的代价呢？或者我们只需把这些病态的细胞控制在危险状态之下？

（2）应访谈数据库管理员，询问数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；数据库记录第 3 级安全测评要求等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除。

4．主机入侵防范访谈

第 3 级安全测评要求主机入侵防范访谈也是 2 项。

（1）应访谈系统管理员，询问是否采取主机入侵防范措施，主机入侵防范内容是否包括主机运行监视、资源使用超过值报警、特定进程监控、入侵行为检测和完整性检测等方面的内容。

（2）应访谈系统管理员，询问入侵防范产品的厂家、版本和安装部署情况；询问是否按要求（如定期或实时）进行产品升级。

5．主机恶意代码防范访谈

第 3 级安全测评要求主机恶意代码防范访谈只有 1 项：

应访谈系统安全管理员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署情况如何，是否按要求（如定期或实时）进行产品升级。

请读者注意，国家标准关于第 3 级主机安全的访谈规定中，没有对“自主访问控制”、“强制访问控制”和“资源控制”的访谈要求（第 4 级以上才出现这几类要求）。

问卷调查表设计：

第 3 章曾介绍了“数据安全访谈问卷调查表”的设计方法。与此类似，在设计“主机安全访谈问卷调查表”的时候，应当将“身份鉴别”、“安全审计”、“剩余信息保护”、“入侵防范”、“恶意代码防范”5 类问卷调查内容包含进去。

在“身份鉴别”访谈中，可以分为操作系统和数据库系统两类基础软件进行身份鉴别的询问。访谈的重点是口令设置、验证码和数字证书等，访谈对象依然是系统管理员、数据库管理员和安全员等。

在“安全审计”访谈中，访谈的重点则是是否配置了主机安全审计设备以及设备的使用情况等。

在“剩余信息保护”访谈中，访谈的重点是磁盘和内存释放空间的技术管理措施是否到位。

在“入侵防范”访谈中，访谈的重点是是否配置了各种专业化的入侵防范设备？配置情况如何？配置的节点数有多少？入侵防护设备的升级制度是否完善？是否有详细的升级记录等。

在“恶意代码防范”访谈中，访谈的重点是杀毒软件的型号（网络版、主机版）、配置情况、升级制度和升级记录等。

表 4.1 是草拟的“主机安全测评访谈问卷调查表”模板，仅供读者参考。

表 4.1　主机安全测评访谈问卷调查表模板

访谈类型	设备型号	访谈内容	访谈对象	备注
身份鉴别	操作系统版本 ☐ Windows 2000/XP/ VISTA ☐ UNIX ☐ Linux Red Hat/红旗 Linux ☐ 其他（请注明）	操作系统身份标识与鉴别机制 ☐ 口令 口令设置策略 ☐ 验证码 ☐ 数字证书（型号、生产厂家等） ☐ 智能卡 ☐ 其他 防止鉴别信息被窃听 ☐ 数据加密技术 ☐ 收/发模型技术 ☐ 数据跟踪监护技术 ☐ 其他	☐ 系统管理员 ☐ 安全检查员 ☐ 安全审计员 ☐ 数据库管理员	
	数据库版本 ☐ Oracle ☐ SQL Server ☐ MySQL ☐ DB2 ☐ 其他	数据库身份标识与鉴别机制 ☐ 数字证书（型号、生产厂家等） ☐ 口令 口令设置策略 ☐ 智能卡 ☐ 其他		
安全审计	主机安全审计设备 ☐ 操作系统/数据库自备审计功能 ☐ 专用安全审计设备 安全审计设备生产厂商 安全审计设备型号、版本	主机系统已采用安全审计 ☐ 是　☐ 否 事件审计的选择与策略（请描述具体的选择方案与策略） 审计日志处理方式 ☐ 定期人工检查 ☐ 事件响应检查	☐ 系统管理员 ☐ 安全检查员 ☐ 安全审计员 ☐ 数据库管理员	
剩余信息保护		操作系统用户的鉴别信息所在的存储空间（磁盘和内存），被释放或再分配给其他用户前是否得到完全清除 ☐ 是　☐ 否 系统内的文件、目录等所在的存储空间（磁盘和内存），被释放或重新分配给其他用户前是否得到完全清除 ☐ 是　☐ 否	☐ 系统管理员 ☐ 安全检查员 ☐ 安全审计员 ☐ 数据库管理员	

续表

<table>
<tr><th>访 谈 类 型</th><th>设 备 型 号</th><th>访 谈 内 容</th><th>访 谈 对 象</th><th>备注</th></tr>
<tr><td rowspan="4">剩余信息保护</td><td rowspan="4"></td><td>数据库管理员用户的鉴别信息存储空间（磁盘和内存），被释放或再分配给其他用户前是否得到完全清除</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>□ 是　□ 否</td></tr>
<tr><td>数据库记录等资源所在的存储空间（磁盘和内存），被释放或重新分配给其他用户前是否得到完全清除
□ 是　□ 否
剩余信息处理方式和策略</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td></td></tr>
<tr><td rowspan="8">入侵防范</td><td>入侵防范设备厂家
□ 启明星辰
□ 绿盟
□ 天融信
□ 其他</td><td>产品升级方式
□ 定期在线升级
□ 事件响应升级
□ 其他</td><td rowspan="8">□ 系统管理员
□ 安全检查员
□ 安全审计员
□ 数据库管理员</td><td rowspan="8"></td></tr>
<tr><td>入侵防范产品型号</td><td>是否采取入侵防范措施
□ 是　□ 否</td></tr>
<tr><td>入侵防范产品版本配置方案和配置节点数目</td><td rowspan="6">入侵防范内容包括
□ 主机运行监视
□ 资源使用超过值报警
□ 特定进程监控
□ 入侵行为检测
□ 完整性检测
□ 其他</td></tr>
<tr><td></td></tr>
<tr><td>配置方案和配置节点数目</td></tr>
<tr><td></td></tr>
<tr><td rowspan="8">恶意代码防范</td><td>杀毒软件生产厂家
□ 瑞星
□ 金山
□ 江民
□ 卡巴斯基
□ 诺顿
□ 其他</td><td>产品升级方式
□ 定期在线升级
□ 事件响应升级
□ 其他
是否采取恶意代码实时检测与查杀措施
□ 是　□ 否
恶意代码实时检测与查杀措施的部署情况</td><td rowspan="8">□ 系统管理员
□ 安全检查员
□ 安全审计员
□ 数据库管理员</td><td rowspan="8"></td></tr>
<tr><td>杀毒软件产品型号</td><td rowspan="6"></td></tr>
<tr><td></td></tr>
<tr><td>杀毒软件版本</td></tr>
<tr><td></td></tr>
<tr><td>配置方案和配置节点数目</td></tr>
<tr><td></td></tr>
<tr><td colspan="2">被测评机构部门名称</td><td colspan="2">部门主管姓名</td><td rowspan="2">访谈日期</td></tr>
<tr><td colspan="2">测评机构部门名称</td><td colspan="2">测评人员姓名</td></tr>
</table>

4.2.2　主机安全现场检查

现场检查的目的是对访谈内容进行核实。这个过程主要包括两个方面的内容：一是对各个主机所对应的相关文档资料进行检查；二是在各型主机上运用各种操作指令进行现场检查。需要指出的是，对于大型信息系统而言，一般都拥有成百上千甚至数千台主机，因此，除非有特殊要求，一般情况下并不需要对所有主机进行逐一检查，而是根据数学中的“抽样理论”进行抽样检查（建议读者参阅任何一本介绍包含有抽样理论的教材）。第 3 级安全测评要求现场检查项共分 8 类 30 项。

1．主机身份鉴别现场检查

第 3 级安全测评要求主机的身份鉴别现场检查共有 5 项。

（1）检查服务器操作系统和数据库管理系统身份鉴别功能是否具有《操作系统安全技术要求》（GB/T 20272—2006）和《数据库管理系统安全技术要求》（GB/T 20273—2006）第二级以上或 TCSEC C2 级以上的测试报告。

这是一个文档检查的工作。一般而言，测评人员在进行该项检查的时候，主要是通过检查当初项目建设的招/投标文件来验证是否达到要求。举例而言，“青天”子系统涉及政府内部办公，巴山市人民政府在招标文件中规定要使用达到国家标准信息安全第 3 级的国产操作系统。那么测评工程师就只需要核对集成商或供货商是否采购了如红旗安全操作系统 2.0 版本，因为该版本已通过中华人民共和国公安部计算机信息系统产品质量监督检验中心的认证，达到第 3 级安全测评的要求。

（2）检查主要服务器操作系统和数据库系统账户列表，查看管理员用户名分配是否唯一。

这是一个“动手检查”的工作，要按照第 3 章所介绍的方法来进行现场检查。

检查目标：检查操作系统管理员账号是否唯一。

检查对象：“青天”子系统 Web 服务器（用于巴山市政府内网网站）。

检查环境：硬件环境包括有高端服务器或普通 PC，512MB 内存，80GB 硬盘，2.99GHz 处理器。操作系统为 Windows 2003。软件环境要无额外增加 Windows 组件，无额外增加其他应用软件（这仅仅是本书模拟环境的要求）。

检查方案：

技术路线

测评人员只需使用 DOS 命令查看操作系统中用户账号管理列表，检查操作系统管理员账号是否唯一。

我们在案例设计中事先设置了两个管理员“ibn”和“pp”。

检查步骤

用鼠标单击“开始”→“运行”模块，然后输入“cmd”指令，进入 CMD 操作控

制台，输入管理员账号查看命令：net localgroup administrators。其输出结果如图 4.2 所示。

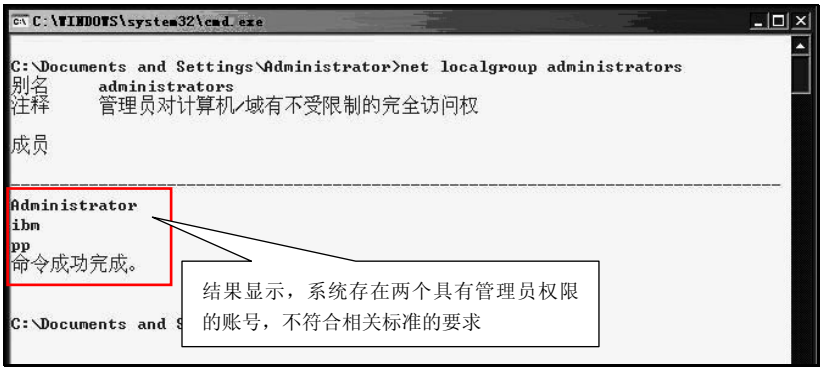


图 4.2　操作系统管理员账号检查

检查结论：该 Web 服务器不符合国家标准关于第 3 级主机身份鉴别的安全测评要求。

（3）检查主要服务器操作系统和主要数据库管理系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点。例如，口令要足够长，口令具有复杂度（如规定字符应包括大、小写字母、数字和特殊字符）等，规定口令生命周期（如每周/每月进行替换等制度要求和替换记录），对新旧口令的替换要求（如规定替换的字符数量）或为了便于记忆使用了令牌。


此项检查可以通过让用户现场输入口令来完成，也可让系统管理员提供相关的口令设置文件和口令替换记录等资料来核对。口令长度至少要达到以 7 个字符以上，并混杂有大、小写字母、数字和特殊符号。对于那些单手甚至单指就可以完成口令输入的用户，要特别关注。对于第 3 级安全等级的主机而言，口令替换记录则应该显示出该被检主机至少每月进行了一次口令替换。

（4）检查主要服务器操作系统和主要数据库管理系统，查看身份鉴别是否采用两个及两个以上身份鉴别技术的组合技术来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合）。

此项检查是在上面检查的基础上的进一步要求，以防止管理员的权限被篡夺之后“门户大开”。检查的方法根据用户所使用的技术/产品而定。例如，若使用数字证书，就可以请使用该证书的用户进行现场操作。同时还需要提醒测评人员注意的是，要核对证书产品（其他产品也是如此）是否通过了国家权威机构的测评认证。

（5）检查主要服务器操作系统和主要数据库管理系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值；查看是否设置网络登录连接超时并自动退出功能。

这是一个可以进行手动检查的项目。模拟的检查流程如下。

检查目标：查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值；查看是否设置网络登录连接超时并自动退出功能。

检查对象：“青天”子系统内网网站 Web 服务器。

检查环境：硬件环境，数据库服务器或普通 PC，512MB 内存，80GB 硬盘，2.99GHz 处理器。操作系统为 Windows 2003。软件环境中无额外增加 Windows 组件，无额外增加其他应用软件。

检查方案：

技术路线

所谓鉴别处理失败功能，取决于该主机所使用的身份鉴别机制。我们仍然以常规性的身份鉴别机制——登录口令作为本检查项的案例分析背景（如果是使用数字证书等产品，可以让该服务器的管理员进行现场错误口令输入等方式来检查，同时要检查数字证书管理制度文件、领用记录等文档资料）。因此，在动手检查的时候主要是使用操作系统现有的“安全设置/账户策略/账户锁定策略”或“安全设置/本地策略/安全选项”这两个模块来查看该服务器 Windows 2003 身份鉴别模块的配置情况。现场检查的重点包括“账户锁定策略”，主机在进行网络连接的时候是否进行了超时限制以及超出了这个时限是否设置了自动退出功能。

检查步骤

① 打开控制面板，依次进入“管理工具”→“本地安全设置”→“账户策略”，然后单击“账户锁定策略”，可以得到如图 4.3 所示界面，如果一个用户登录三次均失败，则该用户就被系统自动锁定。

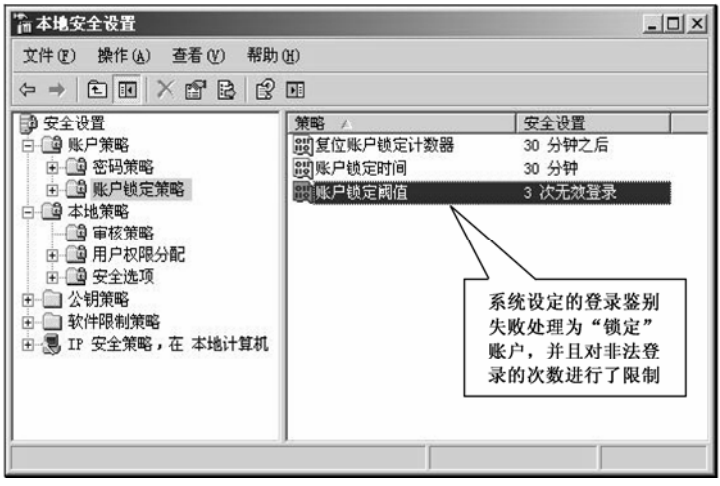


图 4.3　安全设置/账户锁定策略检查

② 在第一步的基础上，打开“本地策略”文件夹，单击“安全选项”，可以看到如

图 4.4 和图 4.5 所示界面。

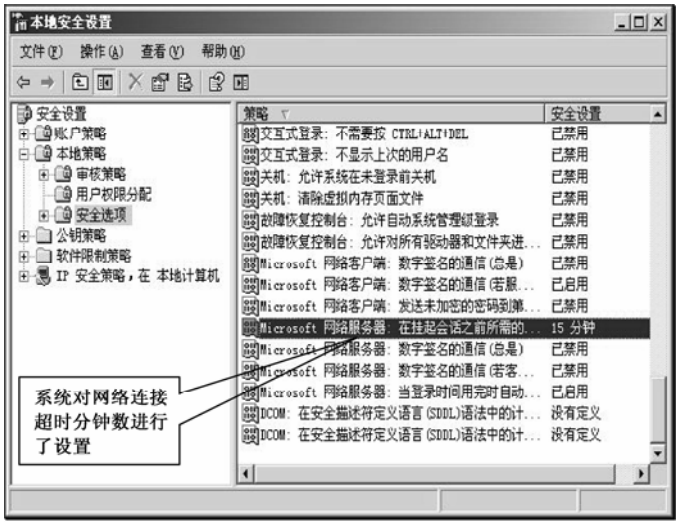


图 4.4　安全设置/安全选项检查（1）



图 4.5　安全设置/安全选项检查（2）

检查结论：该 Web 服务器符合国家标准关于第 3 级主机身份鉴别检查的安全测评要求。

2．主机自主访问控制现场检查

第 3 级安全测评要求主机的自主访问控制现场检查共有 6 项。

（1）检查服务器操作系统和数据库管理系统的自主访问控制功能是否具有《操作系统安全技术要求》（GB/T 20272—2006）和《数据库管理系统安全技术要求》（GB/T 20273—2006）第 2 级以上或 TCSEC C2 级以上的测试报告。

该项检查方法与前面“身份鉴别现场检查”的第一项类似，不再赘述。

（2）检查主要服务器操作系统的安全策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等可能被非授权访问者（人或程序等）进行了限制。

该项检查要求包括了 3 个目标。

检查目标：将上述检查要求分解为 3 个检查子项，包括：①查看重要文件的访问权限是否进行了限制；②查看不需要的服务是否进行了限制；③查看是否对共享路经进行了限制。

我们将给出目标①和目标②的检查步骤，目标③留做练习。

检查对象：“青天”子系统内网网站 Web 服务器。

检查环境：硬件环境，Web 服务器或 PC，512MB 内存，80GB 硬盘等。操作系统为 Windows 2003。

检查方案：

技术路线

对重要文件的访问权限可以通过检查操作系统安全策略模块的配置情况来看它是否对共享的资源访问进行了限制，即查看“共享文件夹”的设置情况；查看不需要的服务是否停止，可以通过查看“服务”模块的配置情况来验证。

检查步骤

① 打开控制面板，依次进入“管理工具”→“计算机管理”→“共享文件夹”，然后单击“共享”，可以得到如图 4.6 所示界面，其中 C、E、F、G 4 个分区的文件均为“默认共享”，因此不符合要求。

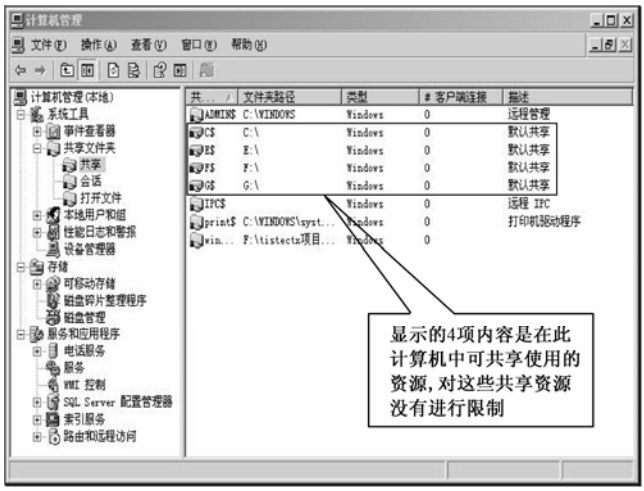


图 4.6　重要文件访问权限检查

② 打开控制面板，依次进入“管理工具”→“服务”，然后查看各项服务的使用状况，可以得到如图 4.7 所示界面。在本案例中，假设 Message 服务不是该被检主机所需要的服务，应该予以禁止。在现场检查的时候所发现的结果与预期相吻合。



图 4.7　本地服务项检查

需要指出的是，对于什么样的服务应该禁止，取决于该主机所处的安全域及所承担的业务等因素。所以，测评工程师需要进行综合考虑并制定与业务相关的安全策略，然后逐一进行检查。一个较好的方法是结合被测机构的业务应用来决定（相关思想方法参见本书后半部分风险评估等章节）。例如，在本案例中，“青天”子系统属于电子政务内部办公系统，那么就应当结合巴山市政府这一级行政单位内部办公的业务需求来确定相关的安全策略。

检查结论：该服务器未对共享资源进行控制，但禁用了不需要的服务，重要文件的访问权限是否进行了限制待定（见本章练习）。

（3）检查主要服务器操作系统和主要数据库管理系统的访问控制列表，查看授权用户中是否不存在过期的账号和无用的账号等；访问控制列表中的用户和权限，是否与安全策略相一致。

下面继续进行动手检查。

检查目标：查看授权用户中是否存在过期的账号和无用的账号。

检查对象：“青天”子系统内网网站 Web 服务器。

检查环境：硬件环境为 Web 服务器或 PC，操作系统为 Windows 2003。

检查方案：

技术路线

该检查项在检查目标中已经讲述得很清楚了，现在只需查看该主机的访问控制列表（ACL）的相关设置即可。至于用户权限是否与安全策略相一致，则需要根据事先确立的安全策略来进行具体分析和判断（见下面第②步的解释）。

检查步骤

① 打开“管理工具”文件夹，进入“计算机管理”，然后查看“本地用户和组”中的

“用户”，可以得到如图 4.8 所示界面（我们在案例设计中将“testuser”定为过期账号）。

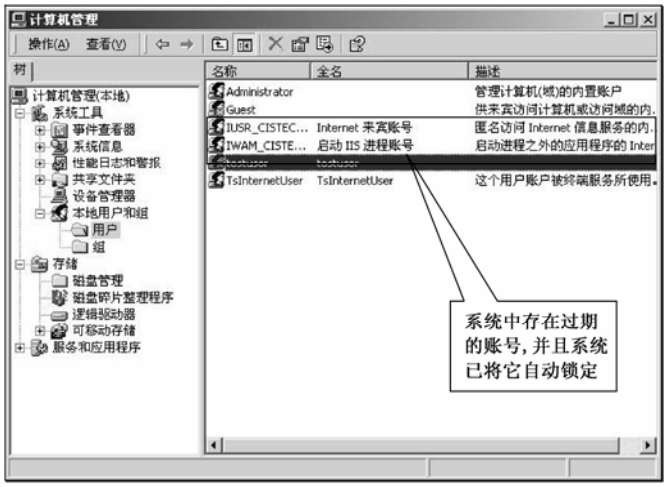


图 4.8　用户账号有效期检查

② 查看用户权限并与安全策略相对比，如图 4.9 所示。

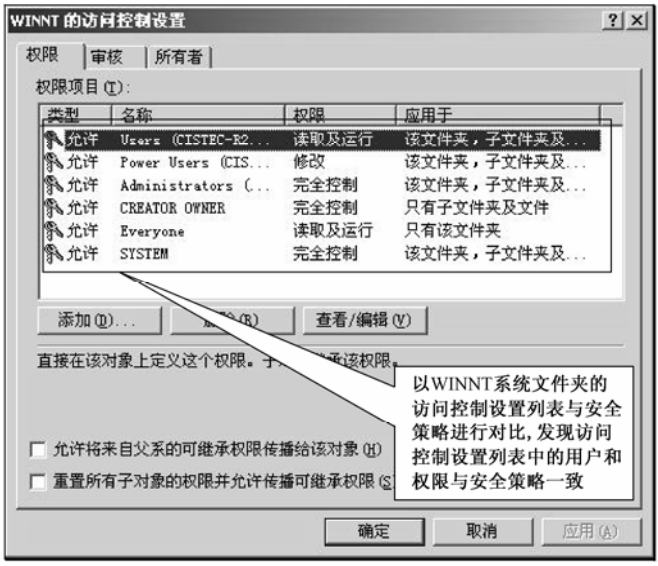


图 4.9　用户权限与安全策略一致性检查

这里需要对上面的安全策略进行一个解释。在“青天”子系统 Web 服务器的安全策略中，有三个用户“Administrators”、“Greater Owner”和“System”拥有“完全控制”的权限。这三个用户分别扮演的是“系统管理员”、“安全管理员”和“安全审计员”的角色，形成了“三权分立”、相互监督的安全机制。而其他用户的权限均比这三员的权限低。所以按照本案例的模拟设计，该主机的自主访问控制是符合要求的。读者在实际工作中则要根据具体情况来判断。有关不同安全员的角色分配，在下面第（4）个检

查项中将再次进行分析。

检查结论：该服务器符合检查条款要求。

（4）检查主要数据库服务器的数据库管理员与操作系统管理员是否由不同管理员担任。


这个要求与银行金库大门必须要两个以上的管理人员才能打开是一个道理。测评人员可以通过核对人员名单并分别询问数据库管理员、操作系统管理员相关的管理技术问题，或查看他们各自的操作来检查该被测单位是否真正做到“两员分离”。当然，在实际工作中，测评人员也要实事求是，应该先确定该被测单位的“主要的数据库服务器”有哪些，然后再进行该条款的现场检查，否则每一台数据库服务器都需要配置不同的人员进行安全管理，既增加了管理成本，在检查工作中也不符合实际情况。

（5）检查主要服务器操作系统和主要数据库管理系统，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员和安全审计员等；查看是否采用最小授权原则（如系统管理员只能对系统进行维护，安全管理员只能进行策略配置和安全设置，安全审计员只能维护审计信息等）。

该条款的检查方法与上面第三条类似，因此留作习题供读者自己进行动手练习。

（6）查看主要服务器操作系统和主要数据库管理系统，查看匿名/默认用户的访问权限是否已被禁用或者严格限制。

检查目标：检查匿名/默认用户的访问权限是否已被禁用或者严格限制。

检查对象：“青天”子系统内网网站 Web 服务器。

检查环境：硬件环境为 Web 服务器或 PC，软件环境为 Windows 2003。

检查方案：

技术路线

匿名/默认用户的访问权限可以通过查看操作系统的安全策略来验证。

检查步骤

进入“控制面板”，找到“管理工具”中的“本地安全策略”，查看本地安全策略中的“安全选项”中的内容。在本案例中，“让每个人权限应用于匿名用户”、“限制匿名访问命名管道和共享”及“允许匿名 SID/名称转换”3 个与匿名访问权限相关的功能被禁止使用（读者在具体工作中可根据实际情况或需求检查其他有关匿名访问的功能是否需要限制，如“可匿名访问的共享”等是否进行了限制），如图 4.10 所示。

检查结论：该服务器符合本条检查要求。

3．主机的强制访问控制现场检查

第 3 级安全测评要求对主机的强制访问控制现场检查共有 3 项，这 3 项均是检查文档资料。

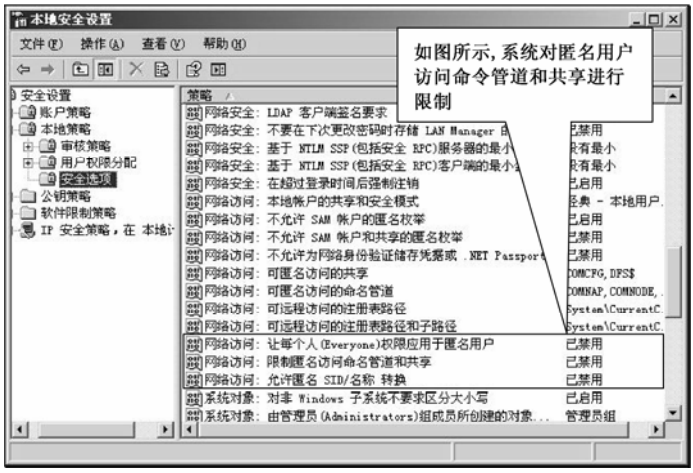


图 4.10　匿名/默认用户访问权限检查

（1）检查服务器操作系统和数据库管理系统的强制访问控制是否具有《操作系统安全技术要求》（GB/T 20272—2006）和《数据库管理系统安全技术要求》（GB/T 20273—2006）第 3 级以上安全测评要求的测试报告。

（2）检查服务器操作系统文档，查看强制访问控制模型是否采用“向下读，向上写”模型，如果操作系统采用其他的强制访问控制模型，则操作系统文档中是否有对这种模型进行的详细分析，并有权威机构对这种强制访问控制模型的合理性和完善性的检测证明。

（3）检查主要服务器操作系统和主要数据库管理系统文档，查看强制访问控制是否与用户身份鉴别、标识等安全功能密切配合，是否控制粒度达到主体为用户级、客体为文件和数据库表级。

4．安全审计现场检查

第 3 级安全测评要求的主机的安全审计现场检查共有 5 项，全部均可进行“动手检查”。下面逐一介绍。

（1）检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看当前审计范围是否覆盖到每个用户。

检查目标：检查操作系统，查看当前审计范围是否覆盖到该机的每个用户。

检查对象：“青天”子系统内部邮件服务器（“青天”子系统的主要功能是一个 OA 系统功能）。

检查环境：邮件服务器操作系统为 Windows 2003。

检查方案：

技术路线

主机的安全审计可以通过专用审计软件来实现，也可以利用本机操作系统所提供的日志审计来验证。在本项检查中，可以通过查看系统管理中的相关设置，如“系统日

志”和“安全日志”来查看其审计范围。在后面的案例中，也将介绍如何使用专用的主机安全审计设备来进行检查。

检查步骤

① 打开控制面板，依次进入“管理工具”→“计算机管理”→“系统工具”→“事件查看器”，然后单击“系统”，可以得到如图 4.11 所示界面。



图 4.11　系统日志覆盖面检查

② 在“事件查看器”下再单击“安全性”选项，得到分别如图 4.12 和图 4.13 所示的界面。

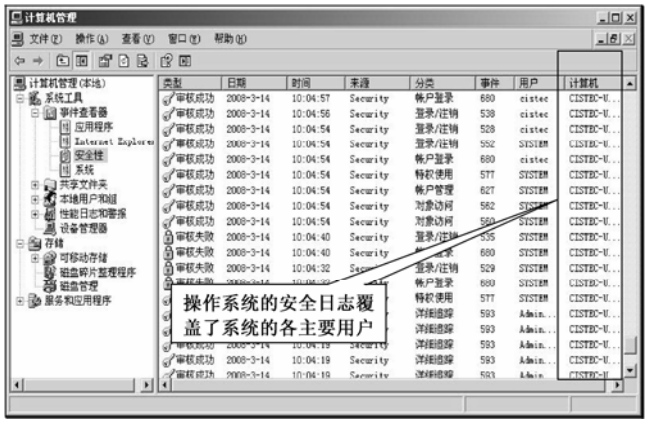


图 4.12　安全日志覆盖面检查（1）

检查结论：该服务器满足主机对用户的安全审计要求。

顺便指出的是，日志查看是一个比较烦琐的工作，本案例分析中的日志分析量和分析指标（只需检查用户级）均较少。如果要查看各种操作的日志，则最好借助于一些日志分析软件（见本书 8.2.3 节）。

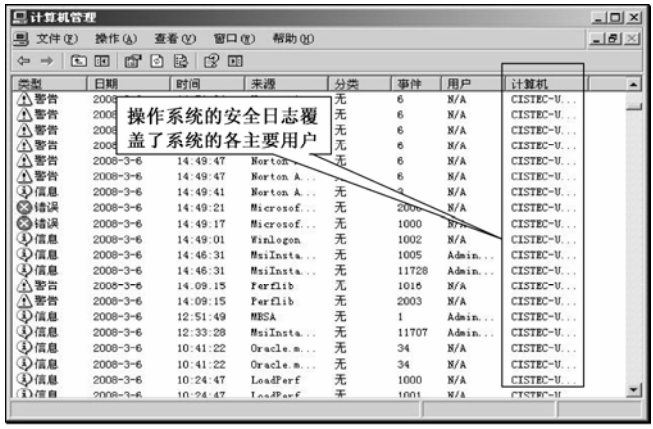


图 4.13　安全日志覆盖面检查（2）

（2）检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计策略是否覆盖系统内重要的安全相关事件。例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用等。

检查目标：检查操作系统，查看审计策略是否覆盖了重要的安全相关事件。

检查对象：“青天”子系统邮件服务器。

检查环境：邮件服务器操作系统为 Windows 2003。

检查方案：

技术路线

这个检查项的关键字是审核策略，需要检查那些重要的安全相关事件，如策略更改、登录、账户管理和特权使用等。而这个模块是操作系统自带的。所以，只需查看系统管理中的相关设置是否配置得当。

检查步骤

打开控制面板，依次进入“管理工具”→“本地安全设置”→“本地策略”，然后单击“审核策略”，可以得到如图 4.14 所示界面，读者可以看到安全审计策略将“审核策略更改”直到“审核账户管理”一共 9 类安全事件囊括其中。

检查结论：该服务器满足第 3 级安全测评主机对安全审计策略的要求。

（3）检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件的成功或失败、身份鉴别事件中请求的来源（如末端标识符）和事件的结果等内容。

该项检查与安全审计现场检查的第（1）项类似，留给读者作为练习。

（4）检查主要服务器和重要终端操作系统，查看是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表。



图 4.14　审计策略对安全事件的覆盖面检查

检查目标：检查操作系统，查看是否为授权用户浏览和分析审计数据提供专门的审计工具。

检查对象：“青天”子系统邮件服务器。

检查环境：邮件服务器的操作系统为 Windows 2003。

检查方案：

技术路线

该检查项与前面通过主机操作系统本身配置的审计模块进行事件检查不同，要求使用专用的主机审计设备（软、硬件均可）来进行“独立”审计。这些产品一般均能满足上述检查条款的要求。

顺便指出的是，目前国内有许多安全生产厂商在进行安全审计产品的研发，市场上也有很多比较成熟的产品，因此读者应该在有条件的情况下（如依托学校的实验室）掌握有关安全审计产品的使用方法，同时也要注意该产品是否通过了国家有关机构的测评认证。为公平、公正起见，本书将不提及我们使用的产品型号，特此说明。

检查步骤

① 进入审计管理界面，如图 4.15 所示，第一列中的“设备信息”和“组信息”等均是指该主机安全审计产品能够进行审计的对象。

② 使用管理界面，选择需要审计的时间段，检查是否能根据需要生成审计统计报表，包括“目标磁盘类型”和“目标磁盘策略”等审计对象以及相应的审计时间（2008 年 3 月 17 日全天），如图 4.16 所示。

检查结论：该服务器安装了专用安全审计工具，并能根据需要进行安全审计报表的生成。



图 4.15　审计记录分类及结果导出检查

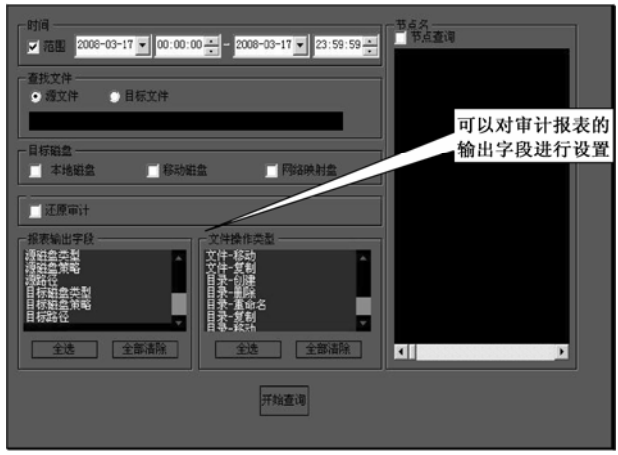


图 4.16　审计时间段及审计统计报表功能检查

（5）检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统，查看审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施。例如，报警并导出、丢弃未记录的审计信息，暂停审计或覆盖以前的审计记录等。

检查目标：检查操作系统和数据库管理系统，查看审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施。

检查对象：“青天”子系统邮件服务器。

检查环境：邮件服务器的操作系统为 Windows 2003。

检查方案：

技术路线

该项检查条款中的各个检查项所要求的模块，均可在操作系统本身的安全设置中找

到，所以还是使用这些现成的安全模块进行检查。建议有条件的读者采用专用审计工具进行检查。

检查步骤

① 打开控制面板，依次进入“管理工具”→“本地安全设置”→“本地策略”，然后单击“安全选项”，可以得到如图 4.17 所示界面，其中“审核：如果无法记录安全审核则立即关闭系统”这一功能被禁用了。



图 4.17　审计跟踪极限阈值设置检查

② 打开控制面板，依次进入“管理工具”→“计算机管理”→“系统工具”→“事件查看器”，然后以鼠标右键单击“应用程序”选项，选择“属性”，可以得到如图 4.18 所示界面，其中对日志大小的上限进行了设置（16384KB），同时设置了达到上限后所采取“按需要覆盖事件”的措施。

检查结论：从测试过程可以看出，当存储空间耗尽不能记录安全审核时，系统会自动采取相应的保护措施“关闭系统”，但该项设置为已禁止，因此测试结果不符合安全审计检查的要求（当然，这是我们故意设置的。用户只需将其设置为“启用”就可达到要求）。而对审计日志则设置了限制，并对超过限制采取了必要的保护措施，因此这项测试结果符合要求。

5．剩余信息保护现场检查

第 3 级安全测评要求对主机的剩余信息保护现场检查共有 2 项，均为文档资料现场检查，其检查方法和重点在前面已多次介绍过，故不再赘述，下面仅列出检查要求。

（1）检查服务器操作系统和数据库管理系统的剩余信息保护（用户数据保密性保护/客体重用）功能是否具有《操作系统安全技术要求》（GB/T 20272—2006）和《数据库管理系统安全技术要求》（GB/T 20273—2006）第 2 级以上的测试报告。

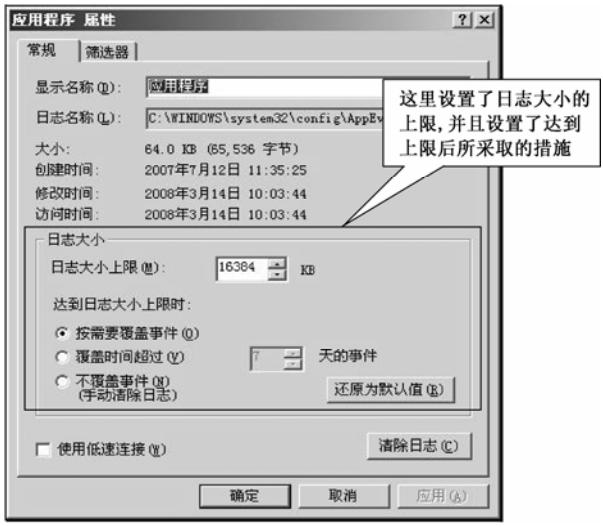


图 4.18　审计日志极限阈值检查

（2）检查主要操作系统和主要数据库管理系统维护操作手册，查看是否明确用户的鉴别信息存储空间，被释放或再分配给其他用户前的处理方法和过程；文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前的处理方法和过程。

6．主机的入侵防范现场检查

第 3 级安全测评要求对主机的入侵防范现场检查共有 3 项。

（1）检查入侵防范系统，查看能否记录攻击者的源 IP、攻击类型、攻击目标和攻击时间等，在发生严重入侵事件时是否提供报警功能（如声音、短信和 E-mail 等）。

检查目标：检查入侵防范系统，查看能否记录攻击者的源 IP、攻击类型、攻击目标和攻击时间等，在发生严重入侵事件时是否提供报警功能。

检查对象：“青天”子系统边界防火墙及内网某终端。

检查环境：防火墙、PC。

检查方案：

技术路线

在实际的现场检查工作中，可以查看安全防护设备的日志来验证是否能够记录攻击者的各种“指纹”（源 IP、攻击目标和时间等）。如果日志上的记录非常干净，则需要采用一些模拟攻击的手段来验证安全防护设备的有效性。当然，模拟攻击必须是在确保系统安全和业务不受任何影响的前提下才能进行。在本书中，我们先扮演“攻击者”的角色，对被监测的主机进行非法扫描，然后通过防火墙的入侵防范功能来实现“青天”子系统中的入侵检测，并通过查看主机防火墙的日志来验证测试目标的内容。

检查步骤

对该主机进行扫描探测（此时保护该主机的防火墙上应有 ICMP 通信记录出现），监

控保护该主机的防火墙日志记录如下，其中攻击危害为“高”，攻击时间为“2007/03/18 10:40:36+8:00…”，源 IP 地址为“192.168.1.1.1.169”，目标地址为“192.168.1.2.139”，攻击类型为“Blocked”，目标 DNS 为“CISTEC-7BC05484”，如图 4.19 所示。



Rating	Date / Time	Type	Protocol	Program	Source IP	Destination IP	Direction	Action Tak...	Co...	Source DNS	Destination DNS
Medium	2007/03/18 10:48:36+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1170	192.168.1.1:139	Outgoing	Blocked	1	CISTEC-7BC05484	
High	2007/03/18 10:41:06+8:00 ...	Firewall	TCP (flags:S)		192.168.1.1:1171	192.168.1.2:139	Incoming	Blocked	1		CISTEC-7BC05484
Medium	2007/03/18 10:41:06+8:00 ...	Firewall	TCP (flags:S)		192.168.1.1:1170	192.168.1.2:445	Incoming	Blocked	1		CISTEC-7BC05484
High	2007/03/18 10:40:36+8:00 ...	Firewall	TCP (flags:S)		192.168.1.1:1169	192.168.1.2:139	Incoming	Blocked	1		CISTEC-7BC05484
Medium	2007/03/18 10:40:36+8:00 ...	Firewall	TCP (flags:S)		192.168.1.1:1168	192.168.1.2:445	Incoming	Blocked	1		CISTEC-7BC05484
Medium	2007/03/18 10:38:08+8:00 ...	Firewall	ICMP (type:8...		192.168.1.1	192.168.1.2	Incoming	Blocked	1		CISTEC-7BC05484
Medium	2007/03/18 10:36:10+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2	192.168.1.1:139	Outgoing	Blocked	1	CISTEC-7BC05484	
Medium	2007/03/18 10:23:46+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1110	[illegible]:139	Outgoing	Blocked	1	CISTEC-7BC05484	
Medium	2007/03/18 10:11:20+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1090	192.16[illegible]	[illegible]	Blocked	1	CISTEC-7BC05484	
Medium	2007/03/18 09:58:54+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1071						
Medium	2007/03/18 09:58:02+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1068						
Medium	2007/03/18 09:57:12+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1066						
Medium	2007/03/18 09:56:20+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1064	192.168.1.1:139	Outgoing	Blocked	1	CISTEC-7BC05484	
Medium	2007/03/18 09:55:30+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1062	192.168.1.1:139	Outgoing	Blocked	1	CISTEC-7BC05484	
Medium	2007/03/18 09:46:38+8:00 ...	Firewall	TCP (flags:S)		192.168.1.2:1047	192.168.1.1:139	Outgoing	Blocked	1	CISTEC-7BC05484	
Medium	2007/03/17 21:27:34+8:00 ...	Firewall	UDP	svchos...	192.168.1.72:1080	202.202.0.33:53	Outgoing	Blocked	1	CISTEC-7BC05484	pridns.cqu.edu.cn
Medium	2007/03/17 19:54:24+8:00 ...	Firewall	UDP	svchos...	192.168.1.72:1354	202.202.0.33:53	Outgoing	Blocked	1	CISTEC-7BC05484	pridns.cqu.edu.cn
Medium	2007/03/17 19:54:24+8:00 ...	Firewall	UDP	svchos...	192.168.1.72:1083	202.202.0.33:53	Outgoing	Blocked	1	CISTEC-7BC05484	pridns.cqu.edu.cn
Medium	2007/03/17 19:54:22+8:00 ...	Firewall	UDP	svchos...	192.168.1.72:1080	202.202.0.33:53	Outgoing	Blocked	1	CISTEC-7BC05484	pridns.cqu.edu.cn
High	2007/03/17 13:05:26+8:00 ...	Firewall	UDP		192.168.0.18:2518	192.168.1.72:137	Incoming	Blocked	1		CISTEC-7BC05484
High	2007/03/17 13:04:56+8:00 ...	Firewall	UDP		192.168.0.18:2370	192.168.1.72:137	Incoming	Blocked	1		CISTEC-7BC05484
High	2007/03/17 13:04:26+8:00 ...	Firewall	UDP		192.168.0.18:2230	192.168.1.72:137	Incoming	Blocked	1		CISTEC-7BC05484

图 4.19　主机入侵防范记录检查

检查结论：从测试过程可以看出，入侵防范系统可以记录攻击者的源 IP、攻击类型、攻击目标和攻击时间等相关重要信息，因此符合检查要求。

（2）检查是否专门设置了升级服务器并实现对重要服务器的补丁升级。

检查目标：检查是否专门设置了升级服务器并实现了对重要服务器的补丁升级。

检查对象：“青天”子系统某专用升级服务器。专用服务器是用于从外网（或公网）上即时获取各种重要补丁信息的设备。它下载了相关的补丁之后，再通过适当的技术（或手工）手段，摆渡到内网的重要服务器或终端上。因此可以有效地防范互联网上的各种攻击直接威胁到内网。但要注意，对这种专用下载补丁的设备要进行特别的安全管理。

检查环境：升级服务器（可用普通 PC 替代）。

检查方案：

技术路线

假设已经配置了一台专用的升级服务器，然后对其进行远程补丁下载（如通过微软的 Software Update Services）。此时，需要在远端计算机上打开 IE 浏览器（5.5 以上版本），然后在地址栏输入“http://服务器名或 IP/susadmin”后回车，接着输入相应的用户名和密码，进行登录。

检查步骤

① 本实验中把服务器的 IP 地址设为：192.168.1.67（可根据自己的实际情况来设置 IP 地址）。

② 通过远程管理在远端计算机（模拟的补丁下载地址）打开 IE 浏览器，在地址栏中输入“http://192.168.1.67”后回车。

③ 输入该地址的主机用户名和登录口令，查看其软件补丁升级的界面，如图 4.20 所示。

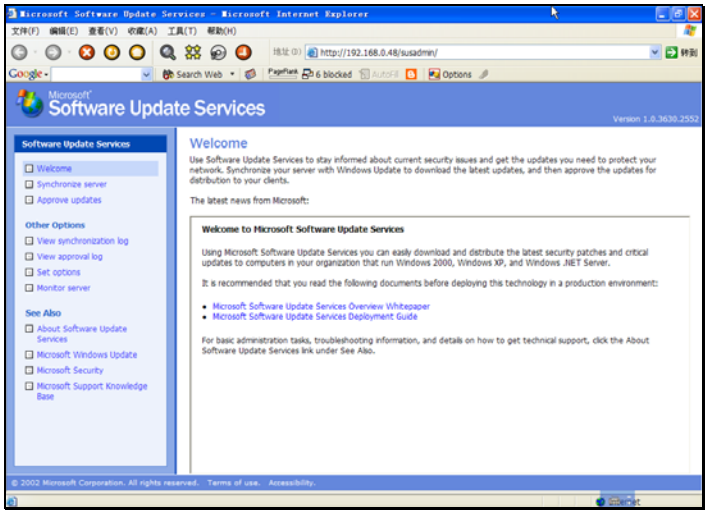


图 4.20　补丁升级服务器检查

检查结论：按第 3 级安全测评要求设置了升级服务器，可以用于对重要服务器的补丁升级，因此符合检查要求。

（3）检查主要服务器是否已经及时更新了操作系统和数据库系统厂商新公布的补丁。

Internet 上肆虐的许多病毒，如进口货“冲击波”、“震荡波”，本土产品“熊猫烧香”等，都是利用了微软操作系统或相关软件的漏洞。因此为了维护自身产品的声誉，微软除了公布一些不得不公布的产品漏洞信息之外，还推出了系列的安全小工具。Microsoft Baseline Security Analyzer（MBSA）就是一款安全状态扫描检测工具。MBSA 能够检测本机上的“微软漏洞”，也可监管我们的“网上邻居”，它还有较为详细的病情检测报告和微软处方（解决方案）。

检查目标：检查服务器的补丁升级情况。

检查对象：“青天”子系统数据库服务器。

检查环境：专用升级服务器和数据库服务器（均可用普通 PC 替代）。

检查方案：

技术路线

这是一个与设置升级服务器实现重要服务器补丁升级的检查项相衔接的检查。可以从微软官方网站上下载 Microsoft Baseline Security Analyzer 补丁升级检查软件并安装到专用的升级服务器上，然后导入内网中的应用终端，再查看对系统升级情况的检查结果。在实际检查工作中，需要检查专用升级服务器是否按照相关的升级工具、下载记录和导入内网终端的记录以及内网终端安装升级补丁的记录等。

检查步骤

① 首先安装 Microsoft Baseline Security Analyzer 补丁升级检查软件。

② 安装成功后运行该软件，单击“scan a computer”扫描项进行扫描。扫描完成后，得到图 4.21 所示界面，从中可以看到“SQL Server Security Updates”、“Windows Security Updates”等新下载的补丁名称及其对这些补丁的概要描述。

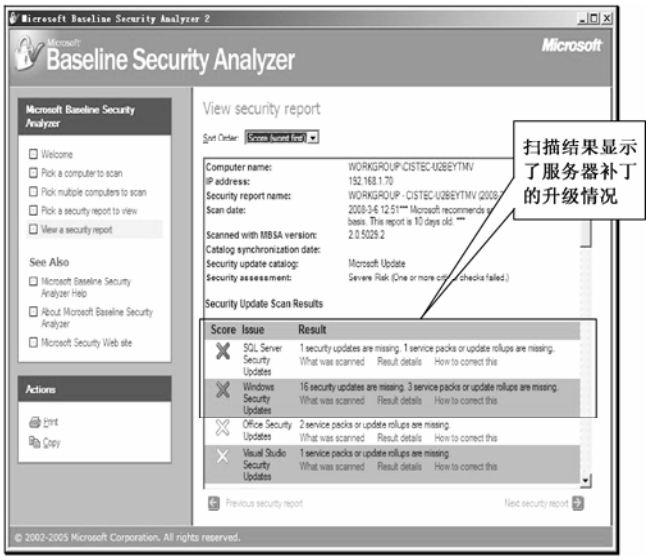


图 4.21　补丁升级情况检查

检查结论：主要服务器对操作系统和数据库系统进行了及时更新，符合检查要求。

7．主机的恶意代码现场检查

第 3 级安全测评要求对主机的恶意代码现场检查共有 2 项。

（1）检查主要服务器系统和重要终端系统，查看是否安装了实时检测与查杀恶意代码的软件产品，查看实时检测与查杀恶意代码的软件产品是否具有支持恶意代码防范的统一管理功能，查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称。

（2）检查网络防恶意代码产品，查看厂家、版本号和恶意代码库名称，查看是否与主机防恶意代码产品有不同的恶意代码库。

下面设计的实验，将把上面两个现场检查要求合二为一进行检查。

检查目标：检查是否安装了实时检测与查杀恶意代码的软件产品，查看实时检测与查杀恶意代码的软件产品是否具有支持恶意代码防范的统一管理功能；查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称。

检查对象：“青天”子系统数据库服务器。

检查环境：数据库服务器（可用 PC 替代）。

检查方案：

技术路线

为了检查是否安装有“实时检测与查杀恶意代码的软件产品”，测评人员可在现场检查的时候通过调阅杀毒软件的日志，对比病毒发现与处理时间等方式来验证。出于安全考虑，本书中通过在模拟环境中进行实时的病毒投送来检查杀毒软件的反应能力，以此来验证测试目标的内容。在此将用对比测试的方式来验证杀毒软件的反应时间。首先，关闭被测主机的杀毒软件，然后输入并激活一个木马程序，通过手工检测的方式检查该木马的存在；然后，启动被测主机的杀毒软件，然后观察被入侵主机中系统杀毒软件产品的反应。

检查步骤

① 先从裸机查看木马程序是否存在（我们事先已经关闭杀毒软件，并植入一个案例木马“Backdoor.devil5.b”），然后在 Windows 命令行状态下输入命令“netstat －a”后，就可以看到目前正在运行的程序所使用的通信端口，其中包括木马程序打开的异常端口，如图 4.22 所示。



图 4.22　异常通信端口检查

② 打开该机“任务管理器”查看进程，如图 4.23 所示。

③ 使用瑞星杀毒软件（或其他通过国家权威机构测评的杀毒软件），发现了该木马

程序“Backdoor.devil5.b”，说明实时检测与查杀恶意代码的功能有效，如图 4.24 所示。



图 4.23　异常进程检查



图 4.24　杀毒软件效果检查

④ 查看该杀毒软件产品的厂家、版本号和恶意代码库名称。测评工程师要注意检查和核对杀毒软件的生产厂家是否在中国授权检测机构，如公安部计算机病毒防治产品检验中心等公布的名单上；版本号是否是最新的，等等信息，如图 4.25 所示。

检查结论：植入的木马程序被本机上的杀毒软件实时发现并进行了查杀，通过该杀毒软件，可以清楚地了解到该杀毒软件的厂家、版本和恶意代码库名称，以及日期等信息。因此，符合检查要求。

8．主机的资源控制现场检查

第 3 级安全测评要求对主机的资源控制现场检查共有 4 项。

（1）检查主要服务器操作系统，查看是否设定了终端接入方式和网络地址范围等条件限制终端登录功能。



图 4.25　杀毒软件产品有效性检查

检查目标：检查主要服务器操作系统，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录功能。

检查对象：“青天”子系统数据库服务器。

检查环境：数据库服务器（可用 PC 替代）。

检查方案：

技术路线

资源控制是一个综合治理的过程。针对本检查条款的要求，先要检测那些无用的用户（会话程序等）是否受到限制，然后查 IP 地址是否可以被进行限制。所以，可以检查“天网”工程系统中的主要服务器的操作系统，通过查看操作系统的组策略编辑器的设置，来验证测试目标的内容。

检查步骤

① 进入操作系统组策略编辑器，依次进入“计算机配置”→“管理模板”→“Windows 组件”→“终端服务”→“会话”，如图 4.26 所示。从图中可以看到已经设置了“为断开的会话设置时间限制”等功能。

② 选择“管理工具”→“本地安全策略”→“IP 安全策略”，双击“安全服务器”选项，在 IP 筛选器列表中，双击所有 IP 通信量，单击“编辑”之后进入“IP 筛选器属性”对话框，如图 4.27 所示。

检查结论：主要服务器操作系统设定了“仅从原始客户端重新链接”和网络地址范围等条件，从而限制了终端登录。因此符合检查要求。

（2）检查主要服务器操作系统，查看是否限制了单个用户对系统资源（如 CPU、内存和硬盘等）的最大或最小使用限度。

检查目标：检查主要服务器操作系统，查看是否限制了单个用户对硬盘的最大或最小使用限度。

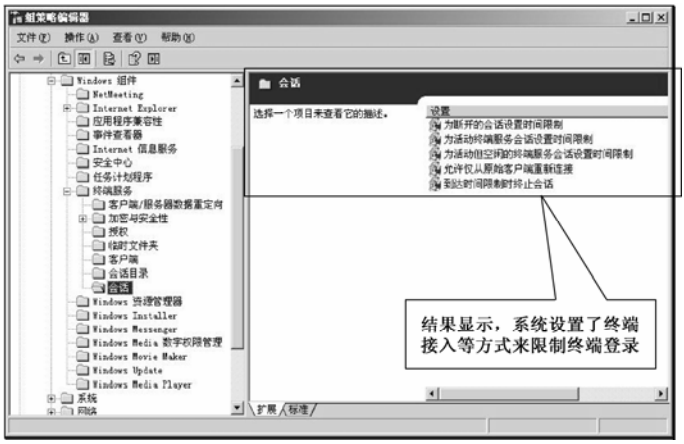


图 4.26　终端登录限制检查

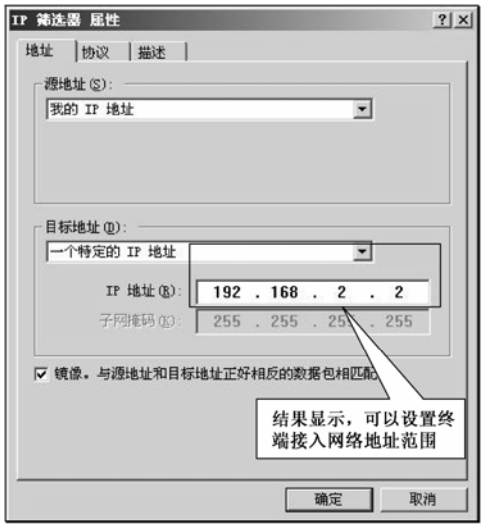


图 4.27　终端接入网址设置检查

检查对象：“青天”子系统数据库服务器。

检查环境：数据库服务器（可用 PC 替代）。

检查方案：

技术路线

单个用户对硬盘的最大或最小使用限度可以通过磁盘配置来进行分配。所以可以通过检查该服务器的操作系统，查看磁盘的属性配置，来验证测试目标的内容。

检查步骤

进入“我的电脑”，以鼠标右键单击需要进行设置的磁盘，然后选择属性。在弹出的属性窗口中选择“配额”选项卡然后单击“配额项”按钮，得到一新界面如图 4.28 所示。



图 4.28　用户对系统资源使用限制检查

检查结论：主要服务器的操作系统设置了用户对硬盘的使用限制，因此符合检查要求。

（3）检查主要服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警。

检查目标：查看系统是否为服务水平设定了最小值；查看是否在服务水平降低到预先规定的最小值时，能进行检测和报警。

检查对象：“青天”子系统数据库服务器。

检查环境：数据库服务器（可用 PC 替代）。

检查方案：

技术路线

操作系统服务水平的下限设置及低于该下限时的报警功能属于操作系统性能设置模块。所以可以通过检查该服务器的操作系统，查看操作系统的性能设置来验证测试目标的内容。

检查步骤

① 打开控制面板，依次进入“管理工具”→“性能”→“性能日志和报警”→“报警”，单击鼠标右键，新建一个报警设置，如图 4.29 所示。

② 打开控制面板，依次进入“管理工具”→“事件查看器”→“应用程序”，双击事件来源为 SysmonLog 的应用程序事件，其显示界面如图 4.30 所示。

从上述内容可见，该机设定了报警操作为执行批处理脚本，该脚本是把出错信息通过 Messager 的形式发送给指定的一台计算机，如图 4.31 所示。

检查结论：主要服务器操作系统为服务水平设定了最小值；服务水平降低到预先规定的最小值时，能检测和报警。因此符合检查要求。

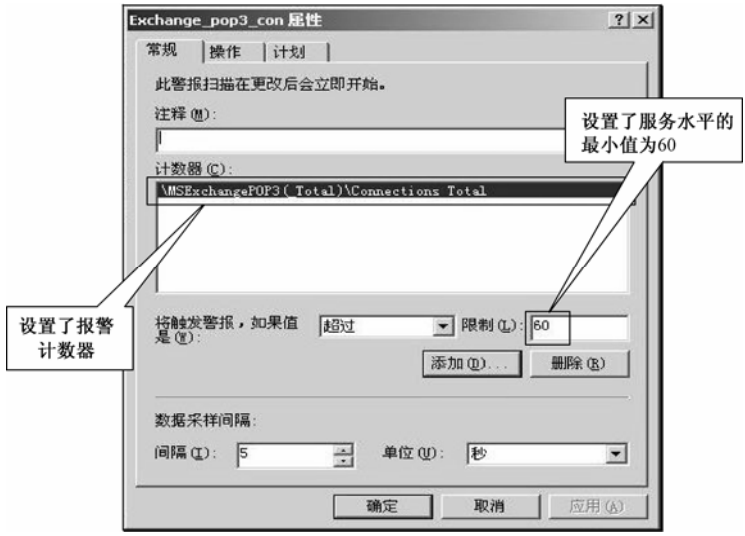


图 4.29　报警功能设置检查



图 4.30　报警阈值启动检查

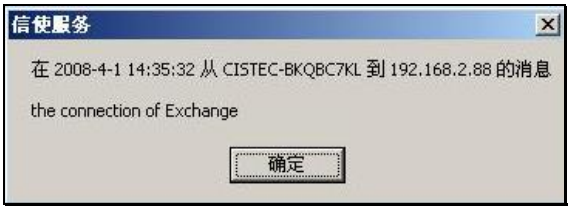


图 4.31　报警信息反馈

（4）检查能够访问主要服务器的终端是否设置了操作超时锁定功能。

检查目标：检查能够访问该服务器的终端是否设置了操作超时锁定功能。

检查对象：“青天”子系统数据库服务器。

检查环境：数据库服务器（可用 PC 替代）。

检查方案：

技术路线

为了检查能够访问该服务器的终端是否设置了操作超时锁定功能，可以现场查看该服务器有关终端服务配置的模块设置情况，并对各种服务进行逐一检查，在本案例中，选择 TCP 服务进行检查。

检查步骤

依次打开“控制面板”→“管理工具”→“终端服务配置”，单击“终端服务配置”，选择“连接”后再双击“RDP-Tcp”，得到如图 4.32 所示界面。

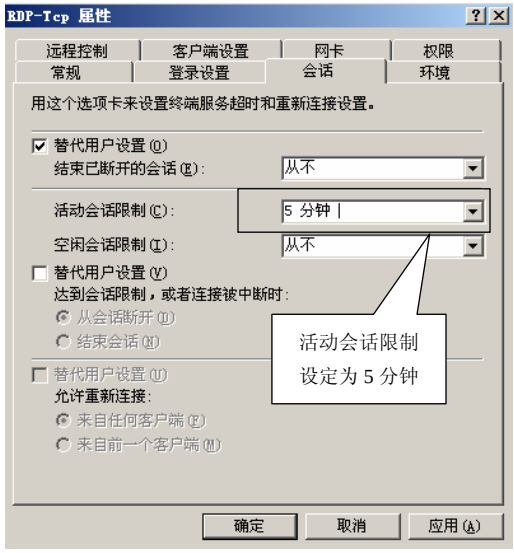


图 4.32　操作超时锁定检查

检查结论：操作超时锁定设定了时间。因此，符合检查要求。

4.2.3　主机安全测试

第 3 级安全测试要求关于主机的安全测试共有 8 项。

请读者回忆一下在“数据安全测试”中，由测评工程师自由发挥的测试项只有 1 项。在主机安全测试中，国家标准则安排了 4 类共 8 个自由测试项，下面分别进行介绍。

1．身份鉴别测试

第 3 级安全测评要求对主机安全身份鉴别测试共有 3 项。

（1）测试主要服务器操作系统和主要数据库管理系统，验证鉴别失败处理功能是否有效。

测试目标：测试主要服务器操作系统和主要数据库管理系统，验证鉴别失败处理功能是否有效。

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

这个测试项实现的方法相对简单，只需通过多次使用错误口令登录系统来测试系统对用户身份鉴别失败的情况，验证测试目标的内容。

需要注意的是，如果系统管理员已经设置了最大登录次数，那么在进行测试的时候要事先询问这个最大值，以免造成系统锁机。如果测评人员要测试这个最大值是否有效，也需要与系统管理员及时沟通。

测试步骤

用一个已有的账户进行错误登录（如乱用口令），连续 3 次登录无效，此时界面如图 4.33 所示。



图 4.33　登录失败次数超过预设值测试

测试结论：连续 3 次使用系统已有的账户进行错误登录，会使账户被锁定。因此，测试结果符合要求。

（2）渗透测试主要服务器操作系统，对服务器操作系统进行用户口令的强度检测，查看能否破解用户口令，破解口令后能否登录进入系统。

攻击者攻击一个目标时常常把破译用户的口令作为攻击的开始。这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。NTCrack 是 UNIX 破解程序的一部分，但是可在 NT 环境下破解。NTCrack 与 UNIX 中的破解类似，但是 NTCrack 在功能上非常有限。请读者注意，如果您没有获得授权就兴致勃勃地去干此类工作，那么您最好事先思考清楚，现实世界中监狱的铁门是不是可以用 NTCrack 破解？

测试目标：渗透测试主要服务器操作系统，对服务器操作系统进行用户口令强度检测，查看能否破解用户口令，破解口令后能否登录进入系统。

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

测评工程师既可以通过现场渗透测试，也可以搭建仿真环境来验证（由于仅仅是服务器操作系统的渗透测试，所以完全可以搭建一模一样的操作系统仿真环境）。为了进行口令强度检测，自然不会用手工方式这种方法（至少不会盲目地使用，而是要使用所谓的“社交工程”手段，这可参阅本书第 12 章），所以应通过使用口令破解工具，测试用户是否使用了（弱）口令，以破解口令后登录进入系统。为了节约实验时间，我们事先设置了一个“123456”的弱口令。在实际的测评工作中，读者会发现有些安全管理不到位的机构或人员大量使用类似的弱口令。

测试步骤

① 首先安装 perl 语言执行环境，下载 NTCrack 口令破解软件。

② 使用 perl 命令行语句启动 NTCrack 工具，如图 4.34 所示。

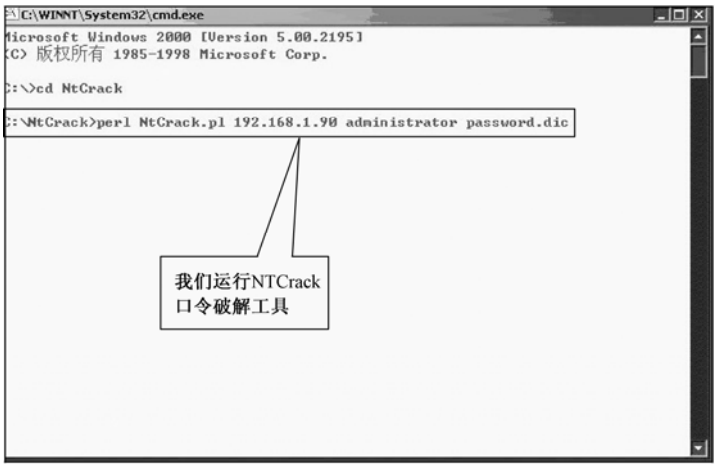


图 4.34　被测主机上运行 NTCrack 工具

③ 获得该机用户口令如图 4.35 所示。

④ 使用破解的口令，成功登录进入系统，如图 4.36 所示。

测试结论：从测试过程可以看出，可以通过使用口令破解工具，获取系统中的弱口令用户名和密码，并使用该账户名和密码成功登录主要的服务器。因此不符合要求。

需要指出的是，一般的口令破解工具主要用于弱口令猜测。事实上有不少社交工程学（Social Engineering）的方法也是有效的（或有害的，见本书“法律、法规”章节），

测试工程师应在测试现场观察是否有用户为了方便起见，将口令写成字条贴在办公桌上等情况。如果发现这种情况则属于非常初级但后果却非常严重的错误。



图 4.35　NTCrack 发现弱口令



图 4.36　使用该弱口令进入被测终端

（3）渗透测试主要服务器操作系统，测试是否存在绕过认证方式进行系统登录的方法，如认证程序存在的安全漏洞、社交工程或其他手段等。

测试目标：测试主要服务器操作系统，测试是否存在绕过认证方式进行系统登录的方法，如认证程序存在的安全漏洞、社交工程或其他手段。

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

为了检验被检主机是否存在绕过认证方式进行登录的漏洞，可以通过监听软件来寻找是否存在没有被系统使用的端口，然后寻找可以绕过系统认证的漏洞。

测试步骤

① 运行 nc.exe 监听一个没有被系统使用的端口，本实验采用 1024 端口，如图 4.37 所示。

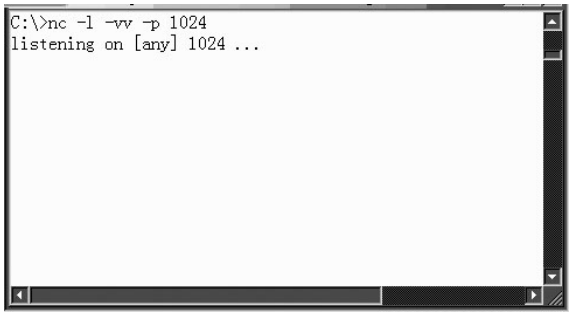


图 4.37　进行端口监听

② 按照如图 4.38 所示的命令格式运行 ms06040rpc.exe。



图 4.38　运行攻击软件 ms06040rpc

③ Nc 监听得到了 shell，说明存在成功的绕过认证方式进行系统登录的情况，如图 4.39 所示。

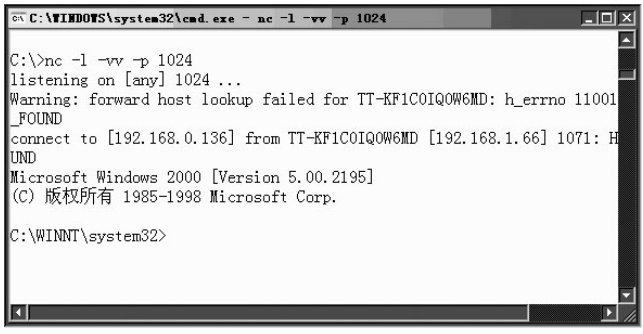


图 4.39　绕过系统认证登录

测试结论：从测试过程可以看出，存在绕过认证方式进行成功系统登录的方法。因此不符合要求。

2．主机的自主访问控制测试

第 3 级安全测评要求对主机安全自主访问控制测试只有 1 项。

测试主要服务器操作系统和主要数据库管理系统，依据系统访问控制的安全策略，并以未授权用户身份/角色进行访问检验，以验证系统是否可以拒绝访问。

测试目标：测试主要服务器操作系统和主要数据库管理系统，依据系统访问控制的安全策略，并以未授权用户身份/角色进行访问检验，以验证系统是否可以拒绝访问。

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

首先以管理员身份登录，查看主要服务器访问控制策略是否严格限制了默认用户的访问权限，然后通过低权限用户越权访问高权限用户方式进行检验，如可以让低权限用户进行系统管理员才能进行的程序安装操作，以验证访问控制策略的有效性。

测试步骤

以管理员身份登录系统，检查用户权限的分配。然后以权限较低的用户身份登录系统。接下来进行越权操作，进行应用程序 AUTORUN 的安装，如图 4.40 所示。由于一般用户只具有 user 权限，因此无法安装程序。

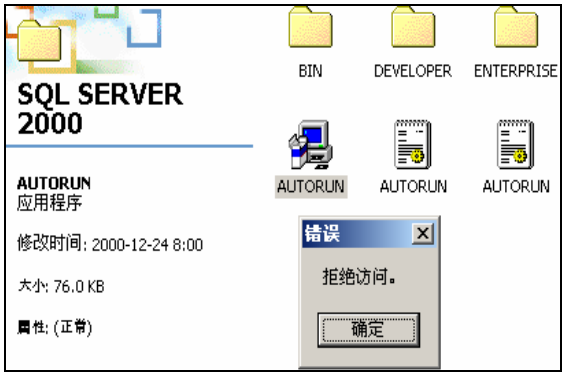


图 4.40　越权操作测试

测试结论：从测试过程可以看出，以权限较低用户身份登录系统，进行越权操作（一般用户只具有 user 权限），无法安装程序。因此，测试结果符合要求。

3．主机的强制访问控制测试

第 3 级安全测评要求对主机安全强制访问控制测试有 2 项。

（1）测试主要服务器操作系统和主要数据库管理系统，依据系统文档描述的强制访

问控制模型，以授权用户和非授权用户身份进行访问，验证是否只有授权用户可以进行访问，而非授权用户不能访问。

测试目标：测试主要服务器操作系统和主要数据库管理系统，依据系统文档描述的强制访问控制模型，以授权用户和非授权用户身份进行访问，验证是否只有授权用户可以进行访问，而非授权用户不能访问。

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

正如本书前面所介绍的，强制访问控制要求按照事先的安全策略对主机进行不可更改的标识。为此需要先进行这类标识的设置，然后再检验非授权用户是否可以对其进行访问。

将主机系统的磁盘分区类型设置为 NTFS；而对重要信息资源和访问重要信息资源的所有主体设置敏感标记；使强制访问控制的覆盖范围包括与重要信息资源直接相关的所有主体、客体及它们之间的操作；并强制访问控制的粒度达到主体为用户级，客体为文件、数据库表级；通过一个用户将 NTFS 分区磁盘上的文件设为私有文件夹，然后以另一个用户的身份尝试访问。

测试步骤

① 以任意用户的身份登录，然后访问不属于 NTFS 分区的文件（任何登录的用户都可以读取不属于 NTFS 分区的磁盘上的文件）。

② 查看设置了访问控制权限的 NTFS 文件，如图 4.41 所示。

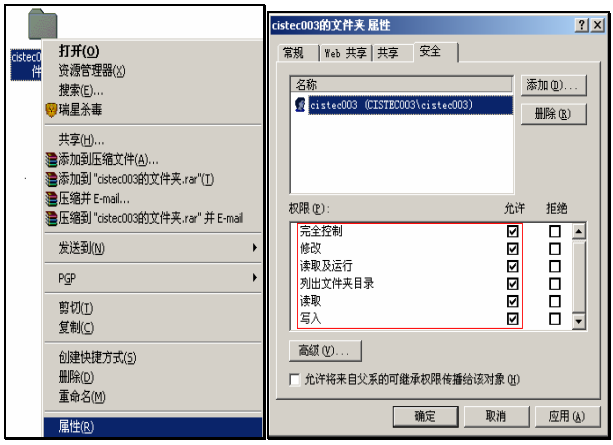


图 4.41　查看设置强制访问控制权限的情况

③ 以其他用户身份登录系统，访问未授权的文件，被拒绝访问，如图 4.42 所示。

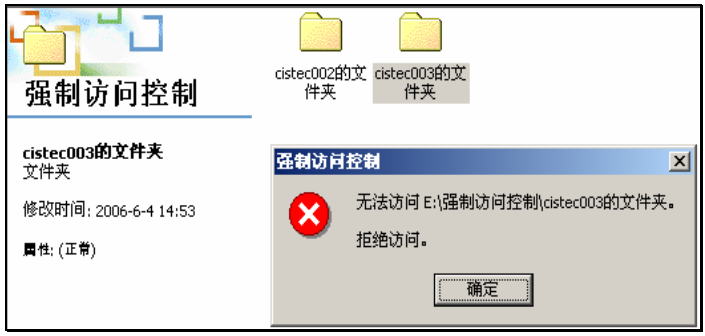


图 4.42　未授权用户访问测试

测试结论：以未授权用户的身份访问设置了强制访问控制的 NTFS 文件，发现只有文件的所有者才有读取和修改文件的权限；以其他用户身份登录系统，访问未授权的文件，被拒绝访问。因此，测试结果符合要求。

（2）渗透测试主要服务器操作系统和主要数据库管理系统，测试强制访问控制是否安全、可靠。

测试目标：渗透测试主要服务器操作系统和主要数据库管理系统，测试强制访问控制是否安全、可靠。

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

为了测试主要服务器操作系统和主要数据库管理系统的强制访问控制是否安全、可靠，可以通过非法终止强制访问模块、非法修改强制访问相关规则、使用假冒身份等多种方式来验证；为了方便读者进行实验，本案例通过非法修改强制访问相关规则，以操作系统普通用户的身份进入系统的“WINNT”属性，以查看其设置来验证测试目标的内容。

测试步骤

以操作系统的普通账户身份来登录系统，进入 C 盘，以鼠标右键单击 WINNT 文件夹，选择属性，如图 4.43 所示。

测试结论：非法修改强制访问相关规则没有操作成功，说明测试的主要服务器操作系统和主要数据库管理系统的强制访问控制安全、可靠，符合要求。

需要指出的是，这个实验所展示的效果仅仅是强制访问控制达到了最低安全限度。换言之，如果能够未经授权地修改该主机的强制访问模块，或者成功假冒授权用户身份等，则说明该项测试没有通过。由此可见，攻防之间的争斗是永远不会停止的……



图 4.43　非法修改强制访问控制策略测试

4．主机的安全审计测试

第 3 级安全测评要求对主机的安全审计测试有 2 项。

（1）测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，验证其审计功能是否受到保护。

测试目标：测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，验证审计功能是否受到保护。

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

选择一台 PC，让其模拟主要服务器或主要数据库管理系统的操作终端，然后通过非法终止审计功能或修改其配置等方式来验证测试目标。

测试步骤

用操作系统的普通账户来登录系统，进入本地安全设置界面，然后尝试对审计配置中的“组策略”进行修改，如图 4.44 所示。

测试结论：用操作系统的普通账户来登录系统，进入本地安全设置界面来对审计配置进行修改，结果显示，系统拒绝普通账户修改组策略，说明用户无法修改审计配置。因此，审计功能受到了保护，符合要求。

（2）测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，验证安全审计的保护情况与要求是否一致。

测试目标：测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，验证安全审计的保护情况与要求是否一致。

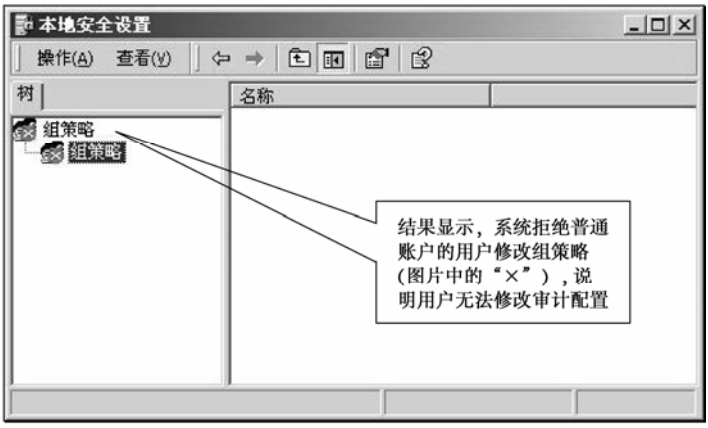


图 4.44　系统设置组策略测试

测试对象：“青天”子系统数据库服务器。

测试环境：数据库服务器（可用 PC 替代）。

测试方案：

技术路线

选择一台 PC，让其模拟主要服务器或主要数据库管理系统的操作终端。然后以操作系统上的一个 guest 用户的身份登录系统，并对审计记录进行删除、修改或覆盖操作，来验证测试目标。

测试步骤

用操作系统的普通账户登录系统后，删除系统的审计日志记录（本实验中我们使用的审计日志为 AppEvent），系统反馈情况如图 4.45 所示。



图 4.45　审计记录删除测试

测试结论：用操作系统的普通账户来登录系统后，无法删除系统的审计日志记录，安全审计的保护情况与要求一致，符合要求。

请读者注意，国家标准对于第 3 级主机安全的“剩余信息保护”、“入侵防范”、“恶意代码防范”和“资源控制”这 4 类，没有测试要求。

最后需要提醒读者注意的收尾工作是撰写《主机安全测评技术报告》，相关要求和方法已在第 3 章中予以阐述。

4.3　本章小结

- 主机安全测评的三种主要方法
- 身份鉴别测评
- 自主访问控制测评
- 强制访问控制测评
- 安全审计测评
- 剩余信息保护测评
- 入侵防范测评
- 恶意代码防范测评
- 资源控制测评

尾声：可信赖的主体

先谈谈我对“可信系统”的“感觉”，然后就你专攻方向的选择给一点建议。

“可信系统”是一个诱人的概念。我们希望，我们的系统是可以信赖的，我们使用它时心里是踏实的，从而使我们有足够的安全感（safety，马斯洛需要层次的第二层，除了基本生存需求之外，安全感就是第一）。

现实中的人造系统，有很多是值得信赖的，比如电视机、电冰箱，以及汽车。但是，软件系统，这个有史以来最复杂的人造物，离“可信赖”标准差得太远，它的结构和它的关系太复杂了，规模太大了，让人感觉难以掌控。但复杂性恐怕只是问题的一个因素，因为“人”作为系统应该具有比软件系统在数量级上更高得多的复杂性，那为什么我们可以对一个特定的人完全信赖呢？这样看来，并非系统复杂就一定不可信赖。系统必须是稳定的、在长期经验中反反复复给人以信心的……软件发展的历史相对短暂，发展又是异常的快（架构范式也就异常地不稳定），因而无法给人以有理有据的和基于经验的信心。所以，我的看法是，“可信赖软件”，只能属于逐渐进化的东西，很可能总是无法达到让人完全满意的地步（简单的软件除外）。

所以，我给你的初步建议是，①把研究范围尽量缩小，同时专深；②能否不拘泥于“理据”或者“理性”的研究角度，而是另辟蹊径，从“经验”的角度去探讨，以“经验”为出发点，同时以“经验”为验证准则？

——摘自一个留德学生的电子邮件

观感

（1）主机安全测评与数据安全测评有什么相同和不同之处？

（2）请完成本章“主机自主访问控制现场检查”第二项内容。设计一个实验来检查主机对重要文件访问权限是否进行了控制。

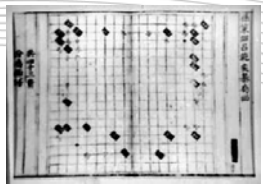
（3）请完成本章“主机自主访问控制现场检查”第五项内容。设计一个实验来检查主机对特权用户的权限是否进行了分离。

（4）请完成本章“主机安全审计现场检查”第三项内容。设计一个实验来检查主机的审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）和事件的结果等内容。

（5）以您所在单位（学校）信息中心为例，撰写一份关于 PC 终端的问卷调查表。

第 5 章
网络安全测评技术





中国古代棋谱——《吴书》

善守者，藏于九地之下；善攻者，动于九天之上，故能自保而全胜也。

——《孙子兵法》（形篇）

序幕：围棋的智慧

“外国用火药制造子弹御敌，中国却用它做爆竹敬神；外国用罗盘针航海，中国却用它看风水；”（鲁迅文集《伪自由书·电的利弊》）。当我们今天有些地方在香烟萦绕、三拜九叩、大兴土木修缮各行各业祖宗的塑像和庙宇，并顺便发展本地旅游业的时候，西方的战略学家们却在深入研究和借鉴我们祖先的智慧之光。

1995 年，美国政府著名智囊机构兰德公司（RAND）的一批资深研究者出版了一本专著（《决战信息时代》，约翰·阿奎拉、戴维·伦菲尔德等著）。书中对信息时代中西方文化进行了精彩的对比分析：

“在美国和欧洲，（国际）象棋常被用来隐喻战争。但对信息时代而言，东方的围棋倒比象棋更能准确地反映冲突的本质。”

“所有的棋子都不分彼此，没有供斩首的王，也没有后方和其他区分。”

“吃掉对方棋子的重要性尚在其次。最终目标在于比对手占领更多的作战空间。”

“它更重视建立由棋子构成的网络，不大重视保护各种级别的棋子。”

“难以区分进攻与防御，一步之举往往既是进攻又是防御。”

“未来的冲突可能更像围棋，而与象棋相去甚远。”

当读者阅读本章之前，您是否思考过什么是网络？什么是网络安全？对这个问题的回答当然是见仁见智（如参见本系列丛书《网络安全概论》）。无论您的答案是什么，只要有人声称他/她的网络是安全的，我们就来测测看！这就是本章的目的。

要点：本章结束之后，读者应当了解和掌握

- 网络安全测评有几个环节？
- 与主机安全的测评手段有何异同？
- 国家标准对于网络安全测评的要求有哪些？

5.1　网络安全测评的诸方面



唉！又是网络安全。在今天信息爆炸的年代，这个名词可能都显得有那么一点“陈旧”了，甚至我们有时把它归为“信息安全”中的“传统安全”领域，而最新出现的“网格安全”、“泛在安全”正在粉墨登场……其实不管名称如何，网络安全的内涵毫无疑问地正在发生新的变化。你看到现在美国陆军的精锐骑兵第一师还在骑马吗？

与前面各章相仿，还是先从简单的思考入手，提一个具有浓厚理想主义色彩的问题：假设每个主机都是安全的，那么由这些主机构成的网络是安全的吗？我们从“个体”和“系统”两个层面来回答，请读者来评判是否正确。一是机器与人一样，总有头痛脑热、“天有不测风云”的时候，随着时间的推移，人的各个器官还会逐渐退化；二是随着业务应用的不断扩展或变化，网络的组成“人员”（人/计算机/硬、软件/工作范围等）也会不断地发生变化。这些变化在给网络注入新鲜血液的同时，也可能带来新的隐患。因此我们认为，即使人类进入了共产主义时代，恐怕也会有网络安全的问题存在。

根据第 2 章中制定的测评工作计划，在对“天网”工程系统（本书案例）完成了“数据安全测评”和“主机安全测评”之后，即将进入网络安全测评阶段。为此，我们来看一看国家有关标准对网络安全的测评又有哪些要求？从管理和技术两个层面，国家标准依然采用“访谈”、“检查”和“测评”3 种手段对网络安全测评提出了若干条款。



2006 年 2 月 6 日至 10 日，美国举行了一场美国历史上最大规模的代号为 “network storm” 的网络战演习。包括国务院、国防部、CIA 等政府部门和微软、思科等 IT 巨头共 115 家机构参与了此次演习。演习模拟的场景是：电力公司的电脑系统受到攻击，导致供电系统失常，并进而导致整个美国能源、运输和医疗系统的瘫痪，从而严重打击公众信心，在美国制造大面积的混乱。在演习中，“攻击方”不断向诸如电力、银行系统等要害部门发起攻击，次数超过 800 次。有趣的是，这次演习将博客也列入重点防范的对象。演习策划者认为，那些在网络日记上大肆灌水的人，尤其是那些经常对时政进行批评的博客们，可能会造成虚假信息的泛滥，从而误导民众……

建议读者在阅读本节的时候多与第 3、4 章的测评条款进行对比，以理解其中的异同。网络安全测评要求中要关注的 8 个方面如下所述。

（1）结构安全与网段划分。热爱大海，梦想扬帆远航的读者可能知道各种舰船都有“水密舱/水密门”这样的结构，以防海水从破损的洞口涌入之后水漫金山。“结构安全与网段划分”的思想与此类似。不过这时“既要防内又要防外”。

（2）网络访问控制。国家与国家之间用边界划分。边界的出入口设置了各种边防检查站、海关等。网络访问控制的基本思想与此类似。这里的“边防检查站/海关”就是各种网络设备的端口等

设施。

（3）拨号访问控制。在某些情况下，网络内部的用户可能需要拨号上网，但前提是需要获得相关的授权。国家标准规定了对单个用户拨号访问的检查，查看网络内每一个用户是否有权使用拨号访问设备。

（4）网络安全审计。这与主机安全审计的思路相仿。

（5）边界完整性检查。在漫长的边境线上，除了设置各种边防检查站对来往人员进行管理检查之外，还要对形形色色的非法越境人员进行监控。

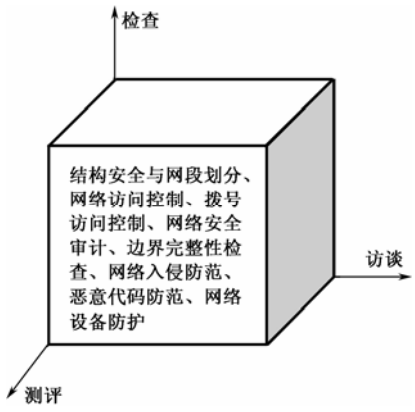


图 5.1　网络安全测评的框架图

（6）网络入侵防范。这与主机入侵防范的思路类似。

（7）恶意代码防范。这与主机恶意代码防范的思路类似。

（8）网络设备防护。这与主机“身份鉴别”的思路类似。

对网络安全进行测评，也是对上述八个方面，利用访谈、检查和测评等手段进行分析。图 5.1 是网络安全测评的框架图。

5.2　网络安全测评的实施

假设现在将对整个“天网”工程系统的基础网络设施展开网络安全测评。由于一个信息系统的基础网络设施是为各个业务应用子系统服务的，如“天网”工程系统的网络设施将为“杜甫”、“青天”等业务子系统提供服务。因此需要开始以下各项工作。

5.2.1　网络安全访谈调研

网络安全访谈调研是国家标准，是以访谈方式进行的。第 3 级安全测评要求对网络安全的访谈分为 8 类 13 项。为了方便读者，本节还增加了问卷调查表设计环节。



这个访谈过程主要是测评工程师与被测评系统的网络管理和技术人员进行问卷式的访谈。当然，在具体工作中，也许您在前面两章“数据安全测评”和“主机安全测评”访谈的对象可能也是网络安全测评访谈的对象。因此您可以根据实际情况灵活掌握。例如，对同一个访谈对象，由同一位测评工程师分别使用“数据安全访谈记录表”、“主机安全访谈记录表”和“网络安全访谈记录表”进行访谈调研。这样既可以提高测评工作效率，也可以降低被访谈人员面对不同测评组时的“烦躁情绪”。

1．结构安全与网段划分访谈

第 3 级安全测评要求对网络安全的结构安全与网段划分访谈共有 4 项。

（1）应访谈网络管理员，询问边界和主要网络设备的性能以及目前业务高峰流量的情况。

（2）应访谈网络管理员，询问网段划分情况及划分的原则；询问重要网段有哪些？其具体的部署位置，与其他网段的隔离措施有哪些？

（3）应访谈网络管理员，询问网络的带宽情况；询问网络中带宽控制情况及带宽分配的原则。

（4）应访谈网络管理员，询问网络设备的路由控制策略有哪些，这些策略设计的目的是什么？

2．网络访问控制访谈

第 3 级安全测评要求对网络安全的网络访问控制访谈共有 2 项。

（1）应访谈安全管理员，询问网络访问控制措施有哪些，询问访问控制策略的设计原则是什么。

（2）应检查边界网络设备，查看其是否根据会话状态信息对数据流进行了控制。

3．拨号访问控制访谈

第 3 级安全测评要求对网络安全的拨号访问控制访谈只有 1 项。

应访谈安全管理员，询问是否允许拨号访问网络；询问对拨号访问控制的策略是什么，采取什么技术手段实现拨号访问控制（如使用防火墙还是使用路由器实现），拨号访问用户的权限分配原则是什么？

4．网络安全审计访谈

第 3 级安全测评要求对网络安全的安全审计访谈只有 1 项。

应访谈审计员，询问边界和主要网络设备是否开启安全审计功能，审计内容包括哪些项？询问审计记录的主要内容有哪些，对审计记录的处理方式有哪些？

5．边界完整性访谈

第 3 级安全测评要求对网络安全的边界完整性访谈只有 1 项。

应访谈安全管理员，询问是否对内部用户私自连接到外部网络的行为及非授权设备私自连接到网络的行为进行监控。

6．网络入侵防范访谈

第 3 级安全测评要求对网络安全的网络入侵防范访谈只有 1 项。

应访谈安全管理员，询问网络入侵防范措施有哪些，是否有专门设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式。

7．网络恶意代码防范访谈

第 3 级安全测评要求对网络安全的恶意代码防范访谈只有 1 项。

应访谈安全管理员，询问网络恶意代码防范措施是什么，询问恶意代码库的更新策略。

8．网络设备防护访谈

第 3 级安全测评要求对网络安全的网络设备防护访谈共有 2 项。

（1）应访谈网络管理员，询问对主要网络设备的防护措施有哪些；询问对主要网络设备的登录和验证方式做过何种特定配置，询问对远程管理的设备是否采取措施防止鉴别信息被泄露，询问对网络特权用户的权限如何进行分配。

（2）应访谈网络管理员，询问网络设备的口令策略是什么。

问卷调查表设计

与第 3、4 两章类似，在设计网络安全现场访谈问卷调查表的时候，将访谈内容分为“结构安全与网段划分”、“网络访问控制”、“拨号访问控制”、“网络安全审计”、“边界完整性检查”、“网络入侵防范”、“恶意代码防范”和“网络设备防护”8 个类别。

在进行“结构安全与网段划分”访谈的时候，重点是“集线器”、“二、三层交换机”、“路由器”、“网关”、“防火墙”等具有网段划分功能的网络设备，同时将这些设备的相关性能指标或参数进行逐一细化。同时，网段的划分方法等也是关注的焦点。访谈的对象是网络管理员。

在进行“网络访问控制”访谈的时候，重点是各种访问控制策略在网络层的执行情况。

在进行“拨号访问控制”访谈的时候，首先关注的是根据被测单位的有关政策，是否运行“拨号上网”。如果允许，再进行更细致的调研，如询问有关拨号访问控制的安全策略，对拨号接入 Internet 等采用何种安全措施等。

“网络安全审计”的访谈可以借鉴第 4 章“主机安全审计”访谈中的思想。访谈对象是单位的安全审计员。

在进行“边界完整性检查”访谈的时候，关注的重点是网络内部非法外连的各种潜在可能，如无线网卡问题等。

在进行“网络入侵防范”访谈的时候，重点是入侵防范设备的适时更新、升级和规范性维护。

在进行“网络恶意代码防范”访谈的时候，重点则是网络版杀毒软件的适时更新、升级和规范性维护。

在进行“网络设备防护”访谈的时候，重点是关心网络关键设备、安全设备的防护措施有哪些（如登录口令、认证令牌等），等等。

表 5.1 是我们建议在测评工作中采用的网络安全调研记录表模板。

表 5.1　网络安全调研记录表模板

访 谈 类 型	设 备 型 号	访 谈 内 容	访 谈 对 象	备注
结构安全与网段划分	边界和主要网络设备	设备性能	网络管理员	
	□ 集线器	□ 传输速率 □ 端口数 □ 网络标准 □ 网络协议 □ 介质		
	□ L2/L3 交换机	□ 交换机类型 □ 传输速率 □ 端口数		
	□ 路由器	□ 固定的广域网接口 □ 固定的局域网接口 □ 路由器类 □ 其他端口		
	□ 防火墙	□ 网络流量 □ 设备类型 □ 用户数限制		
	□ 网关	□ 防火墙性能 □ 最大并发连接数 □ VPN 处理能力 □ 包的转发率		
	□ MODEM	□ 接口类型 □ 传输速率		
	□ 其他			
	业务高峰期流量情况			
	网段的划分情况			
	□ 网段起始地址 □ 子网数 □ 其他			
	网段的划分原则			
	重要网段及保护措施			
	网段 1	保护措施		
	网段 2	保护措施		
	网段 3	保护措施		
	网络带宽情况			
	网络带宽控制情况			
	□ 使用带宽管理软件 □ 代理软件内置的带宽控制功能 □ 通过路由器控制带宽 □ 其他			

续表

访谈类型	设备型号	访谈内容			访谈对象	备注
结构安全与网段划分	带宽分配原则					
	☐ 基于端口的划分 ☐ 基于 MAC 地址的划分 ☐ 基于路由的划分 ☐ 其他					
	网络设备上的路由控制策略措施					
	措施 1		措施目的			
	措施 2		措施目的			
	措施 3		措施目的			
	措施 4		措施目的			
网络访问控制	采取的网络访问控制措施				安全员	
	☐ 执行访问控制列表 ☐ 执行基于网络的访问控制 ☐ 限制远程连接 ☐ 限制无线接入并确保安全 ☐ 启用 Internet 协议安全规则 ☐ 其他					
拨号访问控制	是否允许拨号访问					
	☐ 是　　☐ 否					
	对拨号访问控制的策略是什么					
	☐ QoS 流量预测与流量控制策略 ☐ 网络服务器安全控制 ☐ 其他					
	采取什么技术手段实现拨号访问控制					
	☐ 防火墙技术 ☐ 路由器实现 ☐ 其他					
	采取拨号访问用户的权限分配原则是什么					
	☐ 根据不同用户的角色 ☐ 根据工作的职责 ☐ 其他					
	对保护访问的认证方式有哪些					
	☐ 用户身份认证 ☐ 设备身份认证 ☐ 动态口令认证 ☐ 其他					
网络安全审计	网络系统中的边界和关键网络设备是否设置安全审计功能				审计员	
	☐ 是（包括哪些项）　　☐ 否					
	审计记录的主要内容有哪些					
	☐ 记录时间 ☐ 源地址（IP 和 MAC 地址） ☐ 源端口 ☐ 目标地址（IP 和 MAC 地址） ☐ 目的端口 ☐ 协议类型 ☐ 其他					

续表

访谈类型	设备型号	访谈内容	访谈对象	备注
网络安全审计	对审计记录的处理方式有哪些		审计员	
	□ 存放在永久性介质中			
	□ 存放在数据库中			
	□ 存放在应用程序中			
	□ 其他			
边界完整性检查	是否有对内部用户未通过准许私自连接到外部网络的行为、对非授权设备私自连接到网络的行为进行监控的措施		安全员	
	□ 是（包括哪些措施）　　□ 否			
	网络内“非法外连”的情况			
	□ 使用拨号网路设备非法外连			
	□ 使用无线局域网卡非法外连			
	□ 使用双网卡非法外连			
	□ 使用 GPRS 无线方式非法外连			
	□ 有非法主机或非授权用户读/写涉密文件			
	□ 滥用计算机外围设备			
	□ 通过共享方式泄密			
	□ 安装不明软件或者被植入木马病毒等开启的非法进程			
	□ 其他			
网络入侵防范	网络入侵防范措施有哪些			
	□ 可以安装软件补丁			
	□ 防止后门软件攻击			
	□ 通信加密			
	□ 安装防火墙软件			
	□ 其他			
	是否有专门的设备对网络入侵进行防范			
	□ 是　　□ 否			
	网络入侵防范规则库的升级方式			
	□ 定期在线升级			
	□ 事件响应升级			
	□ 其他			
恶意代码防范	系统中的网络防恶意代码防范措施			
	□ 不轻易访问不了解的网络站点			
	□ 安装网络防火墙			
	□ 及时对系统安装软件补丁			
	□ 及时对防恶意代码病毒库升级			
	□ 其他			
	恶意代码库的更新策略			
	□ 定期在线升级			
	□ 事件响应升级			
	□ 其他			

续表

访谈类型	设备型号	访谈内容	访谈对象	备注
恶意代码防范	防恶意代码产品有哪些主要功能			
	□ 安全策略识别 □ 访问限制 □ 提供网桥式部署方式接入网络的能力 □ 恶意代码的过滤控制 □ 符合规定的加密操作 □ 管理员身份鉴别 □ 管理员权限及管理权限的划分 □ 日志功能 □ 其他			
	系统是否发生过针对恶意代码入侵的安全事件			
	□ 是　　□ 否			
网络设备防护	关键网络设备的防护措施有哪些		网络管理员	
	□ 安装防火墙 □ 安装入侵检测设备 □ 安装防病毒软件，并及时对病毒库进行升级 □ 与网络进行物理隔离 □ 其他			
	对关键网络设备的登录和验证方式做过何种特定的设置			
	□ 远程登录 □ 本地登录 □ 用户身份验证 □ 设备身份验证 □ 动态口令身份验证 □ 其他			
被测评机构下属部门			部门主管姓名	访谈日期
测评机构下属部门			测评人员姓名	

5.2.2　网络安全现场检查

网络安全现场检查过程主要是测评工程师对被测评系统各型网络设备（包括网络安全设备）及其相关文档资料进行检查。对于大型信息系统而言，如果网络设备数量庞大，或者网络覆盖面较广（如包括多个分支机构和机房，并且分支机构的网络设备属于相同型号），则可以在该网络的中心机房进行集中检查。下面分别以“天网”系统的三层交换机、防火墙和入侵检测系统为例，向读者介绍现场检查的主要工作。

第 3 级安全测评要求对网络安全的现场检查共有 8 类 26 项。

1．结构安全与网段划分现场检查

第 3 级安全测评要求对网络安全的结构安全与网段划分检查共有 6 项。

（1）应检查网络拓扑图，查看其与当前运行情况是否一致。

MikroTik Dude 2.0 网络管理器是 MikroTik 新的应用软件，其作用主要通过自动搜索指定子网内的所有设备，绘制和生成网络拓扑图，同时也可用于监视网络中各型设备的服务端口，提供监视和网络分析的功能，并在服务段端口中断后发出警报和提示，记录到当前的日志中。该软件能运行在 Linux Wine 环境、MacOS Darwine 环境和 Windows 下。

检查目标：检查网络拓扑图，查看其与当前运行情况是否一致。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

尽管网络拓扑图的现场检查可以通过人工目视观察的方式来进行，但为了加大拉网检查的力度和粒度，也可以使用各种网络拓扑发现工具来辅助检查工作。因此形成的检查方案是：① 通过网络拓扑设计图纸或网络拓扑设计电子文档来获得该系统规划时的拓扑结构；② 用常用的拓扑扫描工具或者开源拓扑扫描工具来得到当前实际运行的网络拓扑图；③ 更准确的方法是通过检查现有布线来得到当前的拓扑结构，然后将“图上拓扑”与现场拓扑图进行比对（不在本案例分析中，但供读者参考）。

检查步骤

① 用拓扑扫描工具得到当前网络运行拓扑图（图 5.2 是本案例搭建的“天网”系统模拟拓扑图）。读者在使用 MikroTik Dude 2.0 网络管理器的时候，可以先选择“全局网络显示”的模块进行整体网络拓扑情况的核查，然后选择“局部网络显示”模块进行局部网络拓扑情况的检查。

② 然后将该拓扑结构与设计文档中原有拓扑规划结构进行比较。在比较的同时也要核对被测单位制定的网络安全策略是否在网络拓扑结构中得以体现。例如，是否按照“分级、分域，纵深防御”的思想进行网络拓扑的设计与实施等。以“天网”系统为例。由于该系统整体安全等级为第 3 级，但并非意味着它每一个子系统均是第 3 级，如巴山市政府门户网站就不一定按照安全等级第 3 级标准来保护。所以应该通过网络拓扑结构来核对哪些子系统或安全域是属于核心安全域（第 3 级）的，哪些是次要的子系统。这些网络拓扑结构的设计是否体现了分级保护的思想等。

检查结论：通过对用户提供的网络拓扑图与现场检查的结果相对比，可知设计时的拓扑图与现场拓扑图相同（或不同），因此符合（或不符合）检查要求。

（2）检查网络设计/验收文档，查看是否记有边界和主要网络设备业务处理能力、网络接入及核心网络的带宽是否满足业务高峰期的需要，以及不存在带宽瓶颈等方面的设计或描述。

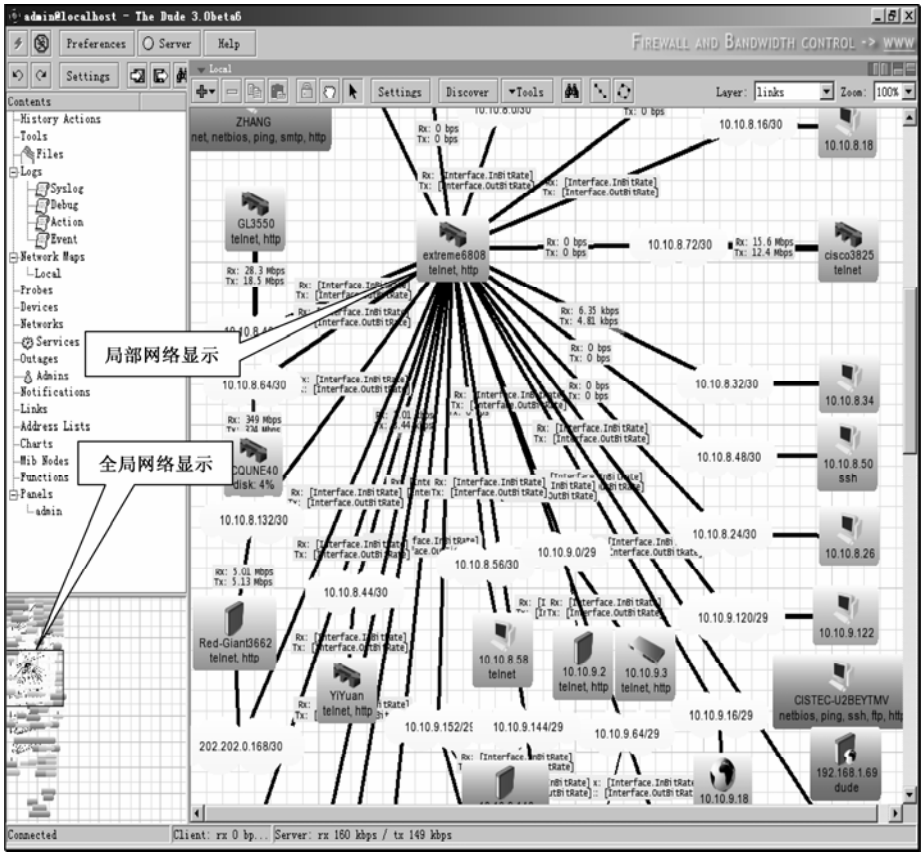


图 5.2　运行 MikroTik Dude 2.0 后绘制的拓扑图

（3）检查网络设计/验收文档，查看是否记有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述。

上面两个检查项均属于文档检查，其方法和检查重点本书前面各章已作过介绍，这里不再赘述。

（4）应检查边界和主要网络设备，查看是否体现了路由控制策略（如使用静态路由等）以建立安全的访问路径。

检查目标：检查边界和主要网络设备，查看是否体现了路由控制策略（如使用静态路由等）以建立安全的访问路径。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

目前，业界常用的路由控制手段分为边界网关、边界防火墙、交换设备和认证隔离设备四种。根据被测单位网络的具体结构和设备情况的不同，可以从四种里面选择对应

的一种或几种设备来进行安全检查。在本书模拟的“天网”大型信息系统中，使用的是一台三层交换设备，因此需要现场查看其路由控制配置。路由控制配置的检查是通过交换设备自带的管理界面来实现的，检查人员只需输入相关的路由追踪指令，即可进行验证。

检查步骤

① 查看路由控制策略是否把重要网段和不安全网段直接连在一起，如果连接在一起说明没有建立安全的访问路径，从而说明该配置策略配置得不合理。

② 查看路由控制策略是否可以使重要网段之间连通，如果没有连通说明配置策略没有建立必要的访问路径，从而说明该配置策略不合理。路由控制策略可以在交换机管理界面中的“Routing”中进行查看，如图 5.3 所示。

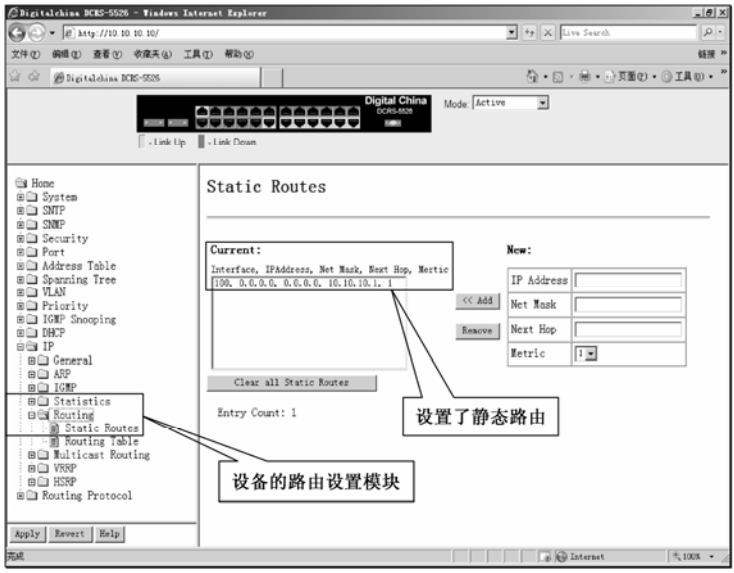


图 5.3　路由控制策略检查（1）

③ 使用路由追踪命令“tracert”检测网络内访问路径是否安全可控。在图 5.4 中我们可以看到，在输入了“tracert 10.10.10.1”的指令之后，得到“Tracing route to 10.10.10.1 over a maximum of 30 hops”和“1　15ms　1ms　1ms　192.168.0.1”（服务器 IP 地址）等的反馈信息，说明网络内部访问路经符合相关策略。

检查结论：该三层交换机配置了静态的安全控制路由，并且通过命令追踪发现该路由是可以追踪并可以控制的。因此该项检查符合要求。

（5）检查边界和主要网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离。

检查目标：检查边界和主要网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

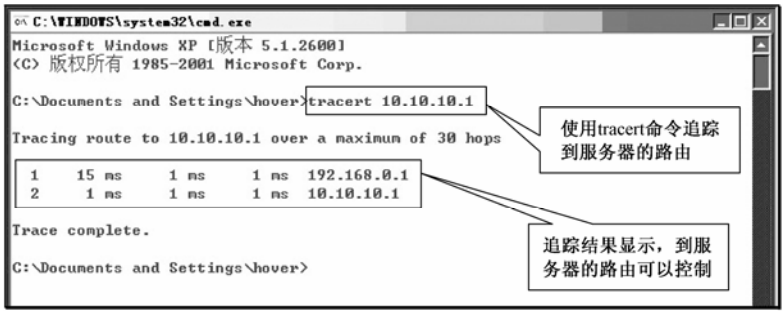


图 5.4　路由控制策略检查（2）

检查方案：

技术路线

目前业界常用的隔离手段分为网闸、防火墙、应用网关、认证隔离设备和交换设备五种。根据单位网络的具体结构和设备情况的不同，可以从这五种手段里选择对应的一种或几种来进行安全检查。在“天网”大型信息系统中，使用的是防火墙设备。

检查步骤

① 查看防火墙设备，其重要网段是否与其他网段直接相连。

② 查看防火墙设备，是否设置了特别规则使重要网段与其他网段的通信得到严格过滤。

③ 检查边界和主要网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离。

④ 检查过程中所绘制的网络边界如图 5.5 所示。从图中可以看出，“天网”系统配置了一台边界防火墙对 Internet 进行逻辑隔离，同时处于“天网”系统内部的另外两台防火墙分别对“业务应用服务器”、“财务应用服务器”和“财务数据库”等核心业务应用区域再次进行了安全隔离。

检查结论：系统的重要网段和网络边界处，均设置了防火墙设备，以防止与危险网段的直接相连，符合检查要求。

（6）检查边界和主要网络设备，查看是否配置了对带宽进行控制的功能，这些功能能否保证在网络发生拥堵的时候优先保护重要业务（如重要业务使用的主机的优先级要高于非重要业务使用的主机）。

检查目标：检查边界和主要网络设备，查看是否配置了对带宽进行控制的功能，这些功能能否保证在网络发生拥堵的时候优先保护重要业务。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

目前，业界常用的带宽控制功能（如路由、交换设备上的 QoS 功能配置情况，专用

的带宽管理设备的配置策略等）分为边界网关、边界防火墙、交换设备和认证隔离设备四种。根据被测单位网络的具体结构和设备情况的不同，可以从上面四种中选择对应的一种或几种设备来进行安全检查。在本书模拟的“天网”大型信息系统中，使用了一台三层交换机，并且通过其管理系统查看端口的速率控制设置情况。

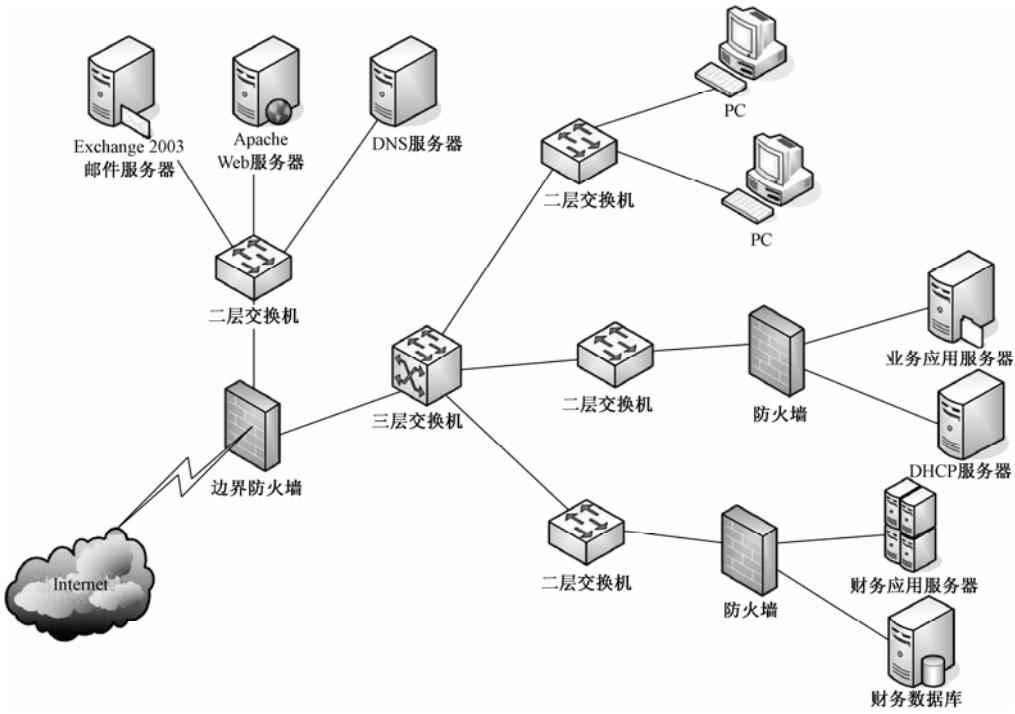


图 5.5　网段隔离检查

检查步骤

① 连接该三层交换机（本例中交换机 IP 为：10.10.10.10）。

② 查看该交换机管理系统中端口的“速率限制”（Rate Limit），如图 5.6 所示。但进入端口速率设置项之后，发现对所有的“Port”（端口）的“Input Rate Limit Status”（交换机入口速率限制状态）下的“Enabled”复选框均未打“√”，所以未进行速率限制。

检查结论：现场检查表明，该三层交换机上没有设置对带宽的限制和管理。因此该项检查未能通过。

2．网络访问控制现场检查

第 3 级安全测评要求对网络访问控制现场检查共有 5 项。

（1）检查边界网络设备，查看其是否根据会话状态信息对数据流进行了控制。

检查目标：检查边界网络设备，查看其是否根据会话状态信息对数据流进行了控制。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

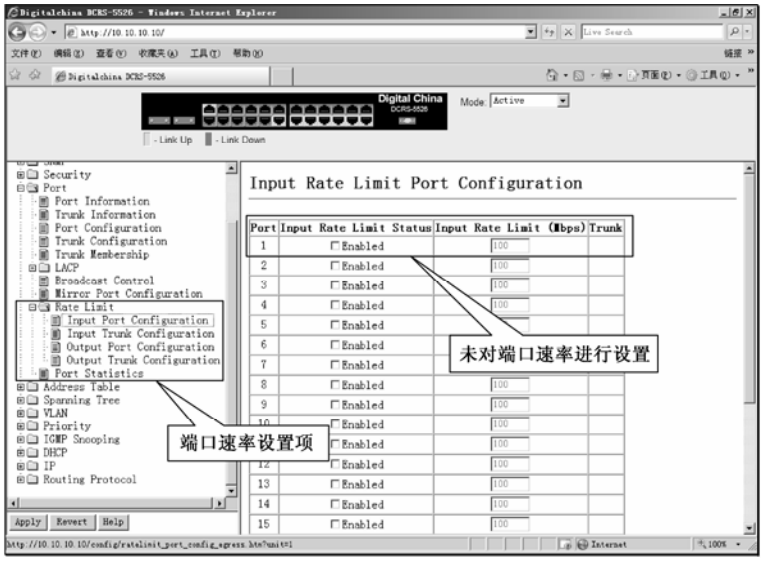


图 5.6　交换机 QoS 设置检查

检查方案：

技术路线

目前常见的能够根据会话状态信息对数据流进行控制的设备有路由设备和防火墙设备等几种。根据被测单位网络的具体结构和设备情况的不同，可以从上面选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中，使用的是防火墙设备。防火墙的检测模块均支持多种协议和应用程序，可用于会话状态信息对数据流的控制。

检查步骤

查看防火墙监测 RPC 和 UDP 等协议的端口信息（包过滤和代理网关都不支持此类端口）。如图 5.7 所示，发现“启动流量控制”这一项未选，说明不能进行流量控制。

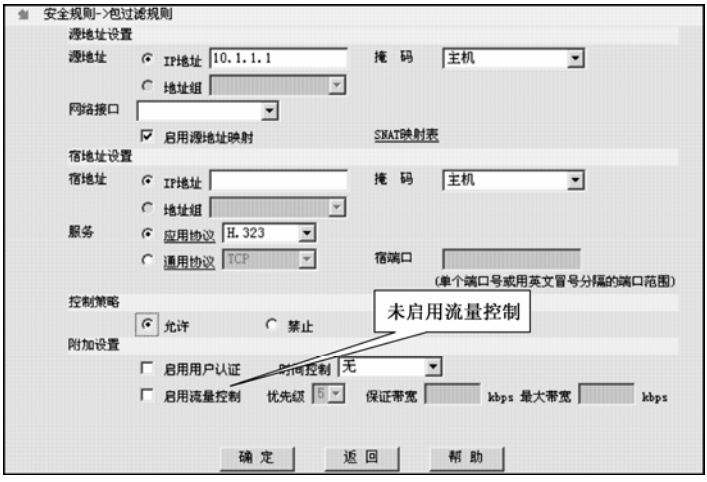


图 5.7　网络边界访问控制检查

检查结论：防火墙上没有设置根据会话状态信息对数据流进行控制功能。因此该项检查未能通过。

（2）检查边界网络设备，查看其是否对进出网络的信息内容进行过滤，以实现对应用层 HTTP、FTP、TELNET、SMTP 和 POP3 等协议命令级的控制。

检查目标：检查边界网络设备，查看其是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP 和 POP3 等协议命令级的控制。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

目前业界能够实现对应用层协议命令级控制的设备有防火墙和路由设备等几种。根据被测单位网络的具体结构和设备情况的不同，可以从上面所述的设备中选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中，使用的是防火墙设备，并通过其管理界面来检查对 HTTP/SMTP/POP3 等协议的控制情况。

检查步骤

通过防火墙配置界面进行设置检查（还可用抓包工具如 Sniffer 等进行验证）时，可以从“服务类型”中看到，能够对 HTTP 和 FTP 等协议进行“用户认证”和“规则策略”等控制，如图 5.8 所示。



图 5.8　协议控制检查

检查结论：现场检查表明，防火墙上设置了对应用层 HTTP、FTP、TELNET 等协议命令级的控制功能，符合检查要求。

（3）检查边界网络设备，查看是否设置了会话处于非活跃的时间或会话结束后自动终止网络连接功能；查看是否设置了网络最大流量数及网络连接数。

检查目标：检查边界网络设备，查看是否设置了会话处于非活跃的时间或会话结束后自动终止网络连接。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

技术路线

目前业界能够实现对网络流量、网络连接和应用层会话管理控制的设备有防火墙和路由设备等几种。根据被测单位网络的具体结构和设备情况的不同，可以从上面所述的设备中选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中，仍然使用防火墙设备来检查。检查内容可分两类：① 是否设置了 QoS 优先级和网络带宽限制；② 是否设置了最大流量数及超过了这个最大值之后是否会自动报警等功能。

检查步骤

以管理员身份登录防火墙设备，查看是否设定了要求的相关配置。从图 5.9 中可以看到，我们对“最大带宽”、“保证带宽”值均设置了限制值。同时，QoS 优先级设置为 3 级。而通过图 5.10 可知，超过连接限制之后，系统在日志中会自动显示报警信息。

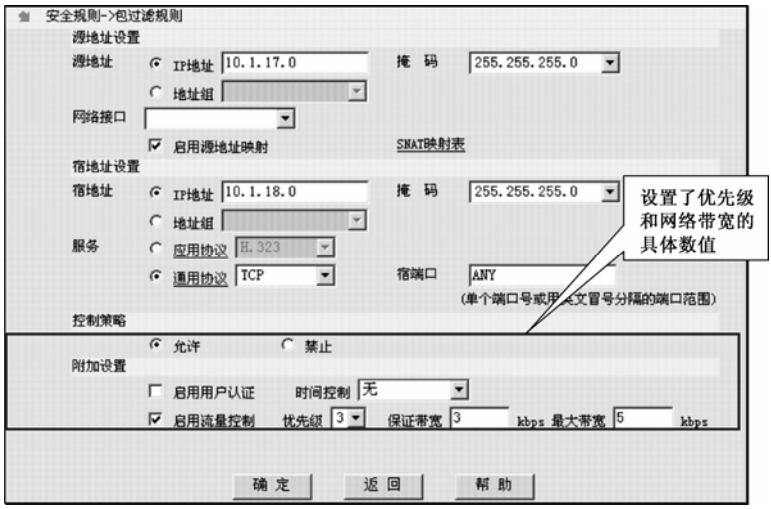


图 5.9　网络服务优先级及带宽设置检查



图 5.10　最大连接数报警设置检查

检查结论：防火墙上设置了网络带宽的最大流量和网络最大连接数，符合检查要求。

（4）检查边界和主要网络设备，查看重要网段是否采取了网络地址与数据链路地址

绑定的措施。

检查目标：检查边界和主要网络设备，查看重要网段是否采取了网络地址与数据链路地址绑定的措施。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

目前业界能够实现对网络地址与数据链路地址绑定的设备有防火墙、路由设备、交换设备、应用网关和认证隔离设备等几种。根据被测网络的具体结构和设备情况的不同，可以从上面所述的设备中选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中，使用的是防火墙设备。因此，需要检查其对重要服务器是否采用了 IP 地址与 MAC 地址的绑定措施。

检查步骤

以管理员身份登录防火墙设备，查看是否设定了相关配置。从图 5.11 中可以看出，IP 地址“10.1.45.234”与 MAC 地址“00:50:BA:CA:9F:2D”之间进行了绑定。

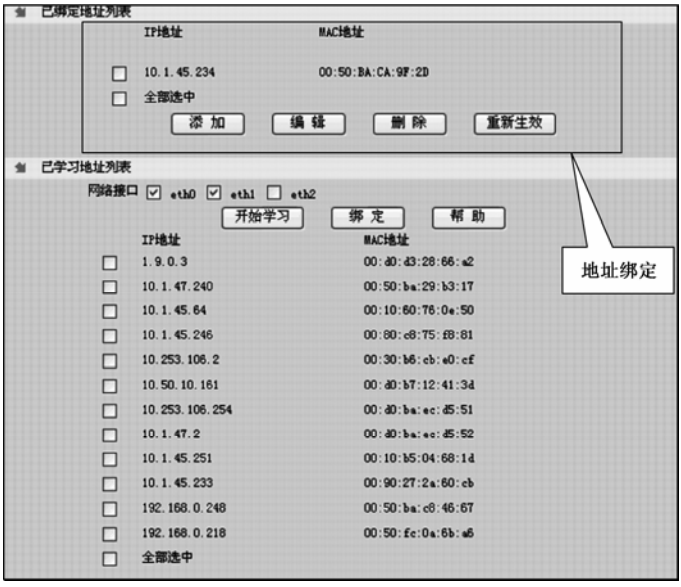


图 5.11　IP 地址与 MAC 地址绑定检查

检查结论：防火墙上设置了对 IP 地址和 MAC 地址的绑定功能，符合要求。

（5）检查边界网络设备，查看是否采取了一定的技术措施防止内部网络信息外泄。

检查目标：检查边界网络设备，查看是否采取了一定的技术措施防止内部网络信息外泄。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

防止内部信息外泄的技术手段有多种，较为普遍的是采用 VPN 技术。目前业界能够防止内部网络信息外泄的设备有防火墙、网络认证隔离设备、网闸、交换机和正在兴起的单向信息导入设备等几种。根据被测网络的具体结构和设备情况的不同，我们可以从这些设备中选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中，使用的是防火墙设备。因此需要检查其 VPN 的设置是否有效。

检查步骤

以管理员身份登录防火墙设备，查看是否设定了相关配置。从图 5.12 中可以看出，该防火墙启用了 VPN 模块，并且设置了共享密钥进行信息加密传输。

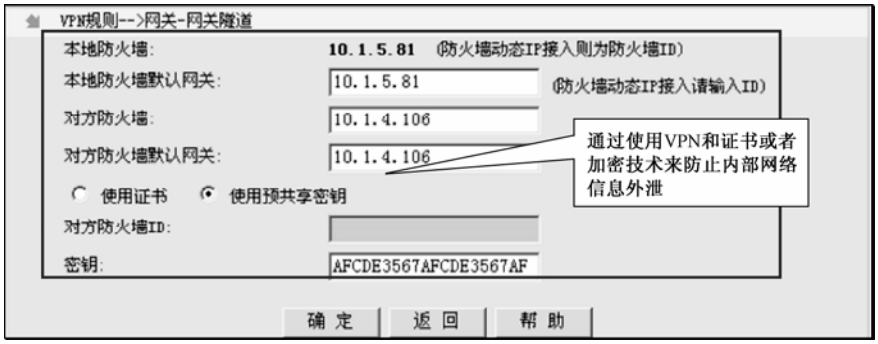


图 5.12　防内网信息泄露检查

检查结论：采用了 VPN 技术手段来防止内部网络信息外泄，符合检查要求。

3．拨号访问控制现场检查

第 3 级安全测评要求对网络安全的拨号访问控制检查只有 1 项。

检查边界网络设备（如路由器、防火墙和认证网关），查看是否正确配置了拨号访问控制列表，其控制粒度是否为单个用户；查看其能否限制具有拨号访问权限的用户数量。

检查目标：检查边界网络设备（如路由器、防火墙和认证网关），查看是否正确配置了拨号访问控制列表，其控制粒度是否为单个用户；查看其能否限制具有拨号访问权限的用户数量。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

目前业界能够实现拨号访问控制的设备有防火墙、网络认证隔离设备、网闸和交换

机等几种。根据被测网络的具体结构和设备情况的不同，可以从上面所述的设备中选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中，使用的是防火墙设备，因此需要检查其对用户数等控制粒度的措施。

检查步骤

① 查看防火墙配置是否有访问控制管理及其控制粒度为单个用户，如图 5.13 所示。



图 5.13　用户控制粒度检查

② 查看具有拨号访问权限的用户数量，发现对该用户数量未进行限制，如图 5.14 所示。

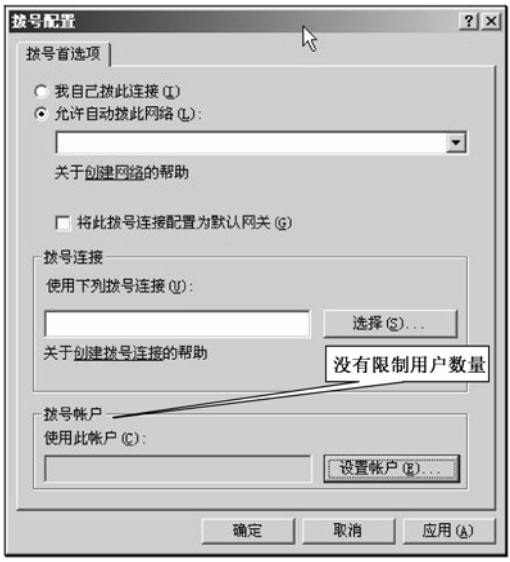


图 5.14　用户数量控制检查

检查结论：在防火墙中已把拨号访问的控制粒度设定为单个用户，但是没有限制具有拨号访问权限的用户数量，因此该项检查只有部分符合要求。

4．网络安全审计现场检查

第 3 级安全测评要求对网络安全审计检查共有 3 项。

（1）检查边界和主要网络设备，查看审计记录是否包含网络系统中的网络设备运行状况、网络流量和用户行为等。

检查目标：检查边界和主要网络设备，查看审计记录是否包含网络系统中的网络设备运行状况、网络流量和用户行为等。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

目前业界能够实现网络边界审计记录的设备有防火墙、边界网关和专用安全审计设备等几种。根据被测网络的具体结构和设备情况的不同，可以从上面所述的设备中选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中，从“普适性”考虑，使用的是防火墙设备。

检查步骤

查看防火墙的相应审计记录是否记录了网络设备运行状况、网络流量和用户行为等。由图 5.15 和图 5.16 所示的审计记录中可见，它给出了 CPU 使用率、内存使用率、当前会话数、最大连接数和接口速率等数据。图 5.17 则展示了我们在操作防火墙时的各种行为及这些操作发生的时间。

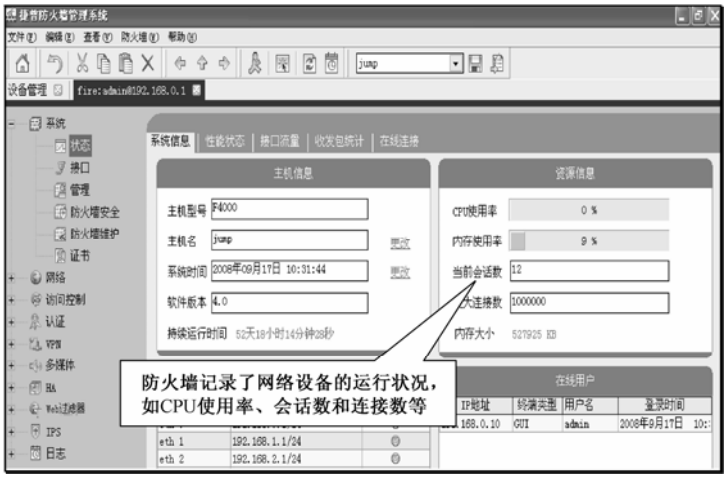


图 5.15　网络运行情况记录检查（1）

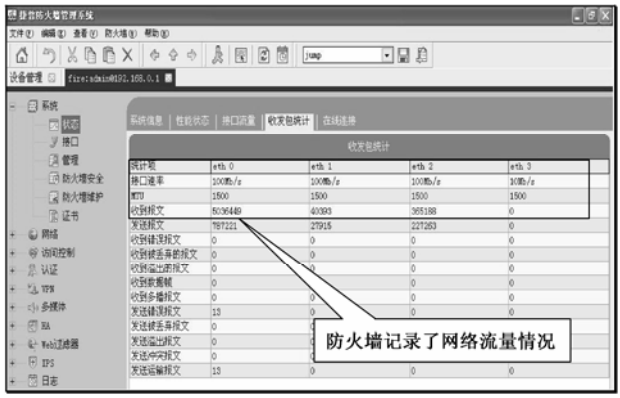


图 5.16　网络运行情况记录检查（2）

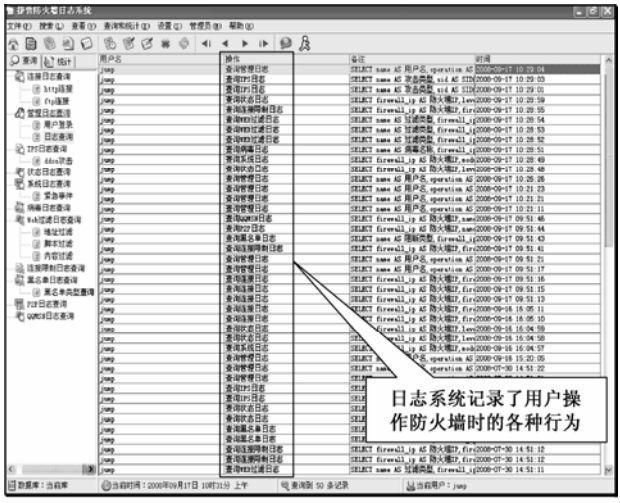


图 5.17　网络运行情况记录检查（3）

检查结论：该测试表明，防火墙的审计记录记录了网络设备运行状况，可以监控用户行为和网络流量，因此符合检查要求。

（2）检查边界和主要网络设备，查看事件审计记录是否包括事件的日期和时间、用户、事件类型和事件成功情况，以及其他与审计相关的信息。

检查目标：检查边界和主要网络设备，查看事件审计记录是否包括事件的日期和时间、用户、事件类型和事件成功情况，以及其他与审计相关的信息。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

此项现场检查要求与上一个检查边界和主要网络设备检查要求有些雷同，但审计内容更细。仍然使用防火墙设备的审计功能来进行检查。

检查步骤

以管理员身份进入审计系统管理界面，查看审计记录，如图 5.18 所示。



序号	时间	日志类型	动作	源地址	目的地址	查看细节
1	9月 28日 09:28:18	管理员操作	SSH admin is off			详细
2	9月 28日 09:28:19	管理员操作	PPP admin is off			详细
3	9月 28日 09:28:22	用户认证	用户认证日志进程启动成功			
4	9月 28日 09:28:22	用户认证	用户认证服务进程启动成功			
5	9月 28日 09:28:22	用户认证	用户认证监控进程启动成功			
6	9月 28日 09:28:22	用户认证	用户认证管理进程启动成功			
7	9月 28日 09:28:25	电子钥匙认证	电子钥匙认证启动			
8	9月 28日 09:29:23	设备事件	设备启动			详细
9	9月 28日 09:29:23	设备事件	设备当	件系统利用率为88%,超过预置的门限		详细
10	9月 28日 09:29:23	设备事件				
11	9月 28日 09:34:19	设备事件				
12	9月 28日 09:34:19	设备事件				
13	9月 28日 09:44:22	设备事件	设备当前的文件系统利用率为89%,超过预置的门限			详细
14	9月 28日 09:44:22	设备事件	设备当前的内存利用率为69%,超过预置的门限			详细
15	10月 15日 11:42:18	管理员操作	SSH admin is off			详细
16	10月 15日 11:42:18	管理员操作	PPP admin is off			详细
17	10月 15日 11:42:22	用户认证	用户认证日志进程启动成功			
18	10月 15日 11:42:22	用户认证	用户认证服务进程启动成功			
19	10月 15日 11:42:22	用户认证	用户认证监控进程启动成功			
20	10月 15日 11:42:22	用户认证	用户认证管理进程启动成功			
21	10月 15日 11:42:24	电子钥匙认证	电子钥匙认证启动			

图 5.18　审计记录覆盖面检查

检查结论：防火墙的审计记录包含了事件的时间、事件类型、事件是否成功等情况，以及其他与审计相关的信息，因此符合检查要求。

（3）检查边界和主要网络设备，查看是否为授权用户浏览和分析审计数据提供了专门的审计工具，并能根据需要生成审计报表。

检查目标：检查边界和主要网络设备，查看是否为授权用户浏览和分析审计数据提供了专门的审计工具（如可以对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

进入中心机房某防火墙管理系统，然后按检查要求查看该防火墙的审计功能。

检查步骤

① 以管理员身份进入审计系统管理界面，查看为管理员提供的浏览和查询工具，如图 5.19 所示，可以看到该防火墙审计系统提供了各种事件，如“入侵攻击事件查询”和“邮件过滤事件查询”等查询模块。同时，也可以通过配置查询时间等方式进行综合统计分析等工作。

② 输入查询条件以后，可以把查询结果以报表的形式显示出来，如图 5.20 所示。

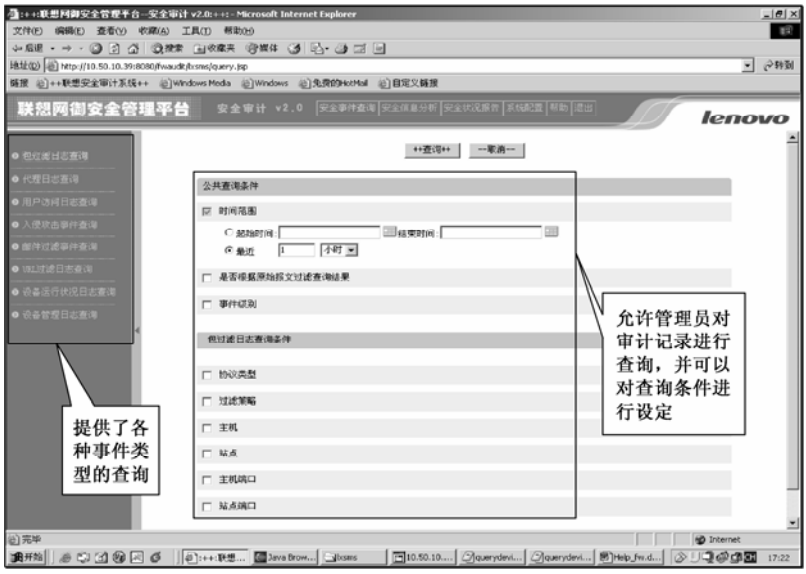


图 5.19　防火墙审计功能模块检查

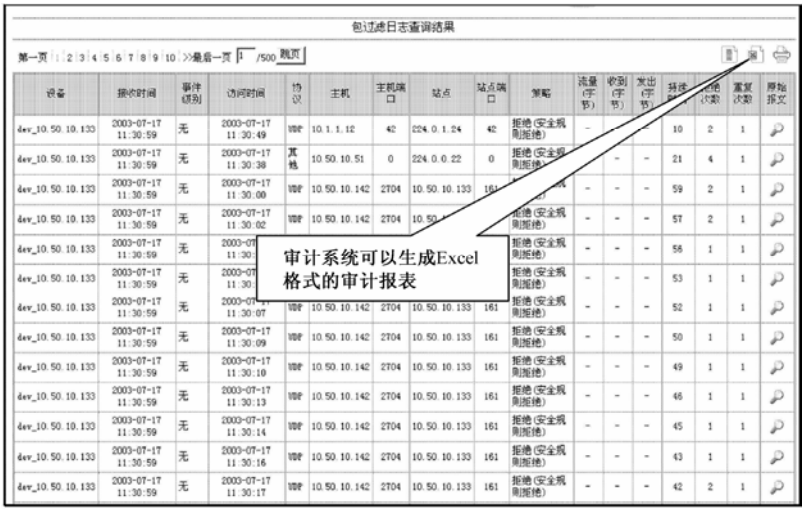


图 5.20　防火墙审计统计报表功能检查

检查结论：防火墙为授权用户浏览和分析审计数据提供了专门的审计工具（如可以对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表，因此符合检查要求。

5．边界完整性现场检查

第 3 级安全测评要求对网络安全的边界完整性检查只有 1 项。

检查边界完整性检查设备，查看是否设置了对非法连接到内网和非法连接到外网的行为进行监控并有效阻断的功能。

检查目标：检查边界完整性检查设备，查看是否设置了对非法连接到内网和非法连

接到外网的行为进行监控并有效阻断的功能。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

进入某防火墙管理系统，检查非法外连阻断设置的情况。

检查步骤

以管理员身份进入防火墙管理设置界面，查看是否设置了对非法连接到内网和非法连接到外网的行为进行监控并有效阻断的功能，如图 5.21 所示。从图中可以看到“正在监视 cistec-4bf2b0f2”，但该防火墙没有设置实时阻断的功能。

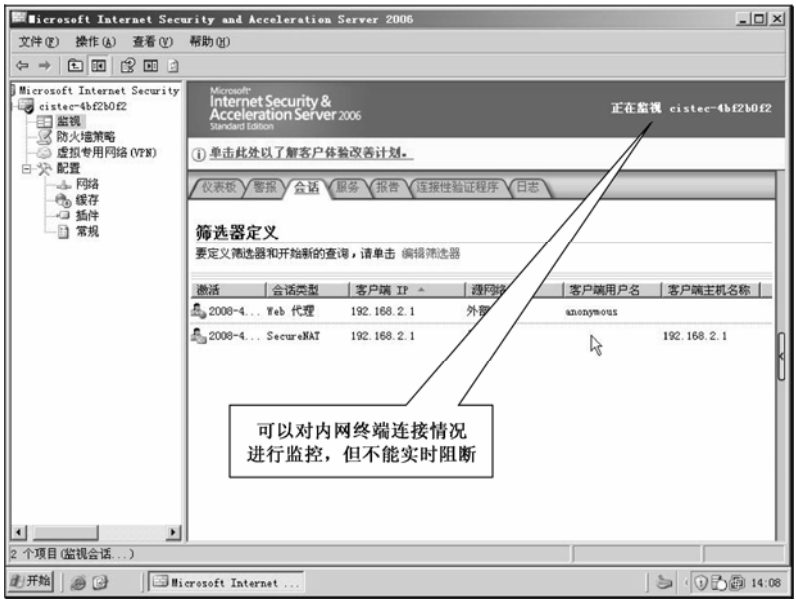


图 5.21　对非法外连阻断设置的检查

检查结论：防火墙提供了对非法连接到内网和非法连接到外网的行为进行监控的功能，但是不能进行实时阻断（可以通过访问策略进行非实时阻断），因此只是部分满足检查要求。

6．网络入侵防范现场检查

第 3 级安全测评要求对网络安全的网络入侵防范检查共有 3 项。

（1）检查网络入侵防范设备，查看是否能检测端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为。

检查目标：检查网络入侵防范设备，查看是否能检测端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

目前许多防火墙产品也具备了成熟的入侵检测功能，所以只需在防火墙的配置管理界面上查看是否有上述各种攻击的检测功能即可。读者也可使用专用的入侵检测设备来进行实验。此外，也可以通过查看日志记录来检验以往是否发生过相关的攻击行为并被防火墙成功拦截。

检查步骤

进入防火墙的入侵检测配置页面，如图 5.22 所示。可以看到图左边第一列罗列了众多的攻击检测模块，如“黑客扫描攻击检测”和“FTP 攻击检测”等，用户可以根据实际情况进行配置。

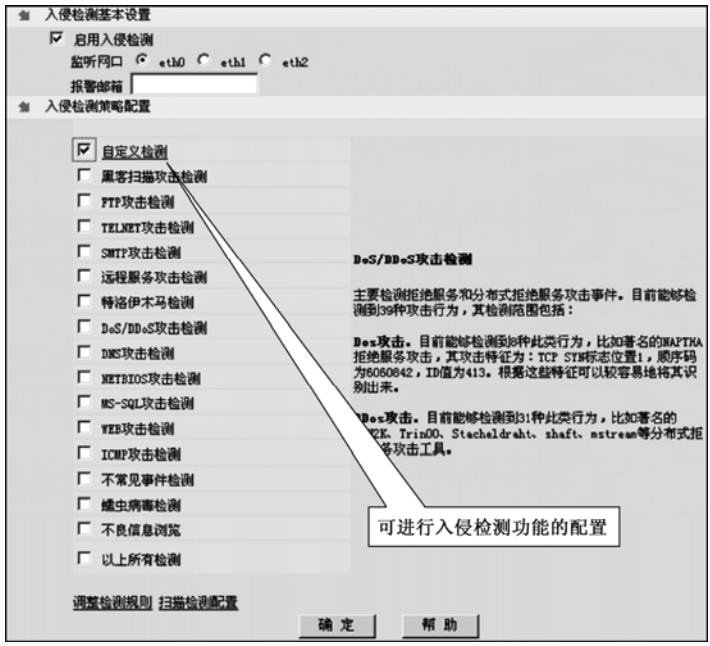


图 5.22　防火墙入侵检测策略配置检查

检查结论：防火墙提供了对端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击的实时检测功能，因此符合检查要求。

（2）检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源 IP、攻击的类型、攻击的目的和攻击的时间等信息。

检查目标：检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源 IP、攻击的类型、攻击的目的和攻击的时间等信息。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

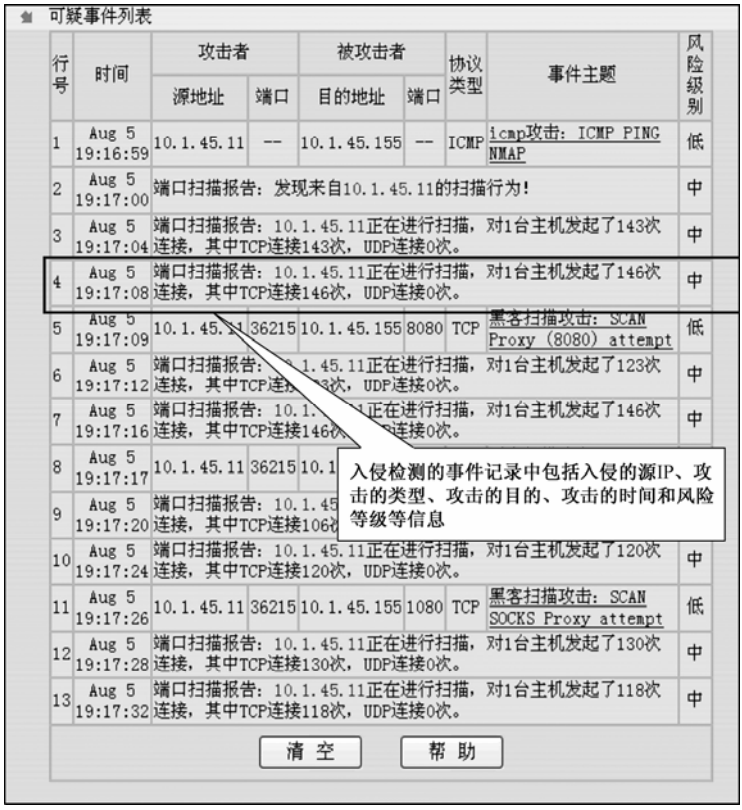
检查方案：

技术路线

在上面的现场检查中，已经对各种入侵检测策略配置进行了检查，为检验这些设置是否真正起到了作用，我们将对这台防火墙发起模拟攻击。

检查步骤

以管理员的身份进入入侵检测系统的管理主界面，首先对入侵检测的攻击类型进行设置，然后对目标机进行模拟攻击。攻击方式选用多种攻击方式从“10.45.1.11”向“10.1.45.155”发起攻击，攻击所采用的协议包括 ICMP 和 TCP 等。现在可以查看如图 5.23 所示的入侵检测的事件记录。



行号	时间	攻击者		被攻击者		协议类型	事件主题	风险级别
		源地址	端口	目的地址	端口			
1	Aug 5 19:16:59	10.1.45.11	--	10.1.45.155	--	ICMP	icmp攻击：ICMP PING NMAP	低
2	Aug 5 19:17:00	端口扫描报告：发现来自10.1.45.11的扫描行为！						中
3	Aug 5 19:17:04	端口扫描报告：10.1.45.11正在进行扫描，对1台主机发起了143次连接，其中TCP连接143次，UDP连接0次。						中
4	Aug 5 19:17:08	端口扫描报告：10.1.45.11正在进行扫描，对1台主机发起了146次连接，其中TCP连接146次，UDP连接0次。						中
5	Aug 5 19:17:09	10.1.45.11	36215	10.1.45.155	8080	TCP	黑客扫描攻击：SCAN Proxy (8080) attempt	低
6	Aug 5 19:17:12	端口扫描报告：1.45.11正在进行扫描，对1台主机发起了123次连接，其中TCP连接3次，UDP连接0次。						中
7	Aug 5 19:17:16	端口扫描报告：10.1.1正在进行扫描，对1台主机发起了146次连接，其中TCP连接146次，连接0次。						中
8	Aug 5 19:17:17	10.1.45.11	36215	10.1				
9	Aug 5 19:17:20	端口扫描报告：10.1.45 连接，其中TCP连接106次						
10	Aug 5 19:17:24	端口扫描报告：10.1.45.11正在进行扫描，对1台主机发起了120次连接，其中TCP连接120次，UDP连接0次。						中
11	Aug 5 19:17:26	10.1.45.11	36215	10.1.45.155	1080	TCP	黑客扫描攻击：SCAN SOCKS Proxy attempt	低
12	Aug 5 19:17:28	端口扫描报告：10.1.45.11正在进行扫描，对1台主机发起了130次连接，其中TCP连接130次，UDP连接0次。						中
13	Aug 5 19:17:32	端口扫描报告：10.1.45.11正在进行扫描，对1台主机发起了118次连接，其中TCP连接118次，UDP连接0次。						中

图 5.23　防火墙对入侵事件的记录

检查结论：防火墙的入侵检测事件记录中包括有对入侵的源 IP、攻击的类型、攻击的目的和攻击的时间等信息的记录，因此符合检查要求。

（3）检查网络入侵防范设备，查看其规则库是否为最新的。

检查目标：检查网络入侵防范设备，查看其规则库是否为最新的。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

该项检查是上一个实验（检查网络入侵防范设备）的收尾工作，重点是查看防火墙的规则库是否可以实时更新，以应对各种新的攻击模式。

检查步骤

登录防火墙配置管理界面后，选择“信息过滤”→“病毒过滤”，便可以进入“病毒过滤模块”的主界面，如图 5.24 所示。可以看到图中有“自动升级”的病毒库版本号模块，但版本号显示结果却是 2001 年。

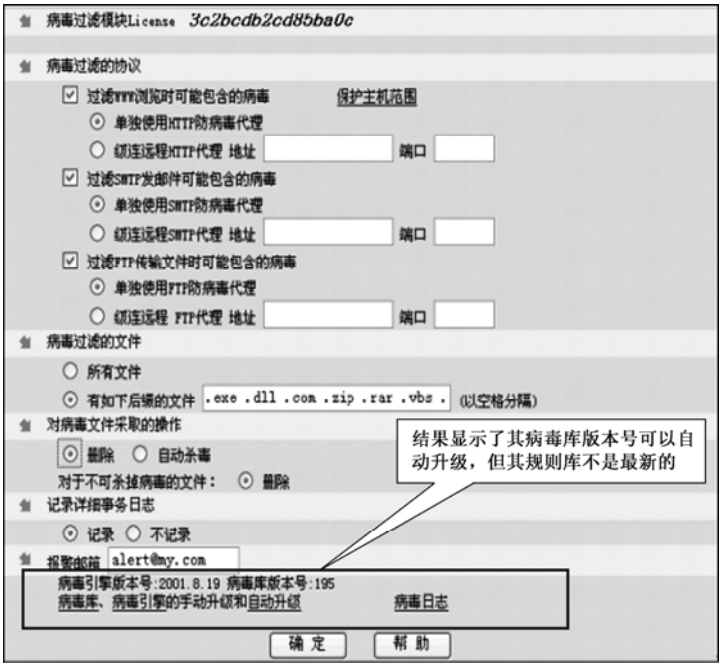


图 5.24　病毒规则库更新检查

检查结论：防火墙的网络入侵模块的规则库不是最新的，不符合检查要求。

7．恶意代码防范现场检查

第 3 级安全测评要求对网络安全的恶意代码防范检查共有 3 项。

（1）检查网络设计/验收文档，查看其是否有在网络边界处对恶意代码采取相关措施（如是否有防病毒网关）的描述，防恶意代码产品是否有实时更新功能的描述。

有关文档现场检查的方法和内容本书前面已多次论及，此处从略。

（2）检查在网络边界及核心业务网段处是否设有相应的防恶意代码措施。

检查目标：检查在网络边界及核心业务网段处是否设有相应的防恶意代码措施。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

这个检查案例应该是许多读者熟悉的操作。只需检查并启动杀毒软件即可。

检查步骤

检查杀毒软件运行情况，如图 5.25 所示。



图 5.25　防病毒软件运行情况检查

检查结论：符合检查要求。

（3）检查防恶意代码产品，查看其运行是否正常，恶意代码库是否为最新版本。

检查目标：检查防恶意代码产品，查看其运行是否正常，恶意代码库是否为最新版本。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

这是上一个检查工作的继续，即查看杀毒软件升级的日志记录。

检查步骤

查看杀毒软件更新日志记录，如图 5.26 所示。

检查结论：防恶意代码产品运行正常，恶意代码库为最新版本，符合要求。



图 5.26　杀毒软件版本更新检查

8．网络设备防护现场检查

第 3 级安全测评要求对网络安全的网络设备防护检查共有 4 项。

（1）检查边界和主要网络设备，查看是否配置了对登录用户身份的鉴别功能，口令设置是否有复杂度要求；查看是否能对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

检查目标：检查边界和主要网络设备，查看是否配置了对登录用户身份的鉴别功能，口令设置是否有复杂度要求；查看是否能对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

检查边界和主要网络设备的现场检查要求是对网络边界防护设备本身进行身份鉴别检查。其操作过程与主机身份鉴别检查类似，但其验证流程更细，这是因为边界防护设备本身就应当是高安全的。

检查步骤

① 打开防火墙后，程序提示用户输入 PIN 码（初次使用 PIN 码为“123456”），然后单击“确定”按钮，如果正确，屏幕将显示如图 5.27 所示的对话框，即对管理员的身份进行验证。其中右上角的交通灯有三种状态：红灯表示还未通过防火墙认证，黄灯表示正在等待防火墙认证，绿灯表示已经通过认证。分别如图 5.27 和图 5.28 所示。



图 5.27　登录防火墙



图 5.28　防火墙身份认证检查

② 检查口令设置是否有复杂度要求。在本实验中，通过修改密码查看对口令的设置，发现没有复杂度的要求，为了使系统更具有安全性，建议在实际应用中采用复杂口令，以加强其安全性，如图 5.29 所示。



图 5.29　防火墙登录口令复杂度检查

③ 查看是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。电子钥匙用于对防火墙管理员的身份认证，此处采用双因子认证的方式，除了需要普通的用户认证信息外，还限定一把钥匙只能根据其存储的防火墙 ID 访问一台特定的防火墙，如图 5.30 所示。

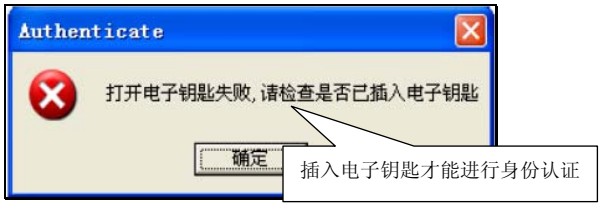


图 5.30　防火墙多因素身份鉴别检查

检查结论：该防火墙配置了登录用户身份鉴别功能，但口令设置没有复杂度要求；对同一用户有两种鉴别技术来进行身份鉴别，因此只是部分符合检查要求。

（2）检查边界和主要网络设备，查看是否配置了鉴别失败处理功能。

检查目标：检查边界和主要网络设备，查看是否配置了鉴别失败处理功能（如是否有鉴别失败后锁定账号等措施）。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

本检查工作属于网络设备防护检查中第（1）项检查的继续，因此读者应当针对同一种边界防护设备进行检查。只需多次使用错误口令进行登录，然后观察其反应就可以达到该项检查的目的。

检查步骤

① 用错误的口令进行登录，检查是否会把错误登录账号进行锁定或者系统对其连接进行强制断开，如图 5.31 和图 5.32 所示。



图 5.31　错误口令登录检查（1）



图 5.32　错误口令登录检查（2）

② 查看是否有限制非法登录次数的功能，并连续三次输入错误口令，此时通过电子钥匙进行身份鉴别失败，防火墙登录自动退出，如图 5.33 所示。

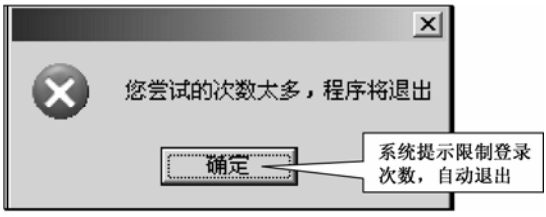


图 5.33　错误口令登录检查（3）

③ 重新登录防火墙，以防火墙认证用户身份连接防火墙，当登录信息不正确时，系统自动与服务器通信中断，如图 5.34 所示。



图 5.34　错误口令登录检查（4）

检查结论：该防火墙设置有鉴别失败后锁定账号的功能，符合检查要求。

（3）检查边界和主要网络设备，查看是否配置了对设备远程管理所产生的鉴别信息进行保护的功能。

检查目标：检查边界和主要网络设备，查看是否配置了对设备远程管理所产生的鉴别信息进行保护的功能。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

本案例中可继续使用网络设备防护检查中前面两项检查使用的防火墙进行实验。对于进行实际检查工作的测评人员而言，则要根据用户信息网络的具体情况来决定抽检哪一台设备。

检查步骤

远程登录主要网络，输入用户名和密码。如果输入了错误的用户名和密码，可以看到主要网络拒绝登录，鉴别信息保护功能是有效的，如图 5.35 所示。

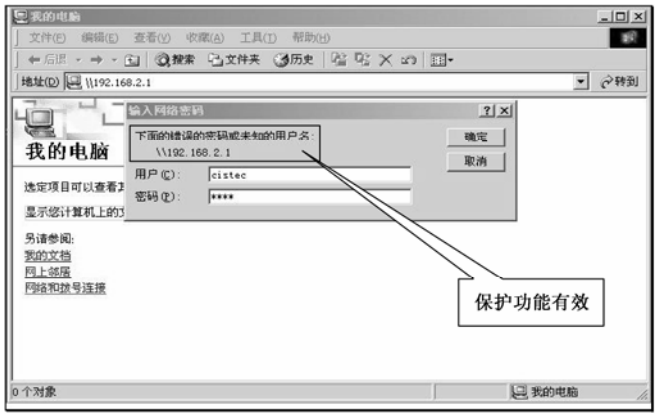


图 5.35　远程用户鉴别信息检查

检查结论：该防火墙配置了对设备远程管理所产生的鉴别信息进行保护的功能，因此符合检查要求。

（4）检查边界和主要网络设备，查看是否对边界和主要网络设备的管理员登录地址进行了限制；查看是否设置了网络登录连接超时并自动退出功能；查看是否实现了设备特权用户的权限分离。

检查目标：检查边界和主要网络设备，查看是否对边界和主要网络设备的管理员登录地址进行了限制；查看是否设置了网络登录连接超时并自动退出功能；查看是否实现了设备特权用户的权限分离。

检查对象：“天网”系统中心机房。

检查环境：“天网”系统中心机房。

检查方案：

技术路线

首先查看防火墙是否对管理员登录地址进行了限制；然后对管理员主机（即管理防火墙的主机）地址进行设定，同时对防火墙管理的主机进行地址设定，再重新登录防护墙查看是否对管理员登录地址进行了有效限制。接下来检查网络登录连接超时的设置情况（可将超时时间值设置得较小，然后现场检验是否发挥作用）。最后设计两个用户来检验对特权用户是否进行了权限分离。

检查步骤

① 查看防火墙是否对管理员登录地址进行了设定，如图 5.36 所示。由此可以知道管理员登录时是要受口令和地址的限制的。

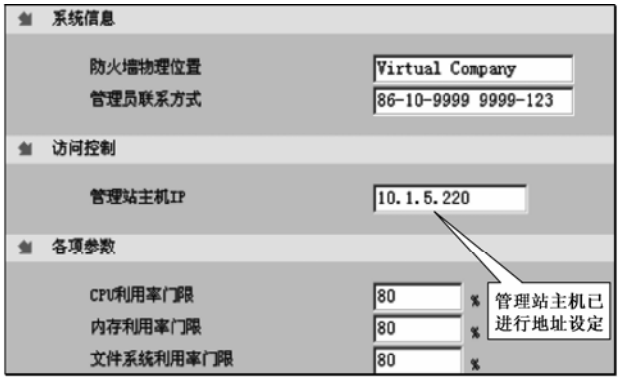


图 5.36　管理员登录地址设置检查

② 对边界和主要网络设备的管理员登录地址进行设置，验证对登录地址限制的有效性。为此，设置管理防火墙的 IP 地址为：10.1.5.200，如图 5.37 所示。



图 5.37　防火墙管理终端 IP 地址设置检查（1）

③ 设置防火墙管理的主机 IP 地址为：10.1.5.201，如图 5.38 所示。

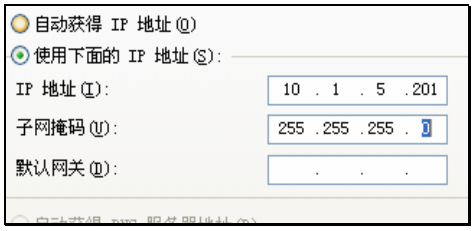


图 5.38　防火墙管理终端 IP 地址设置检查（2）

④ 重新登录防火墙，如图 5.39 所示。



图 5.39　普通用户登录限制检查

⑤ 查看是否设置了网络登录连接超时并自动退出功能，如图 5.40 所示。

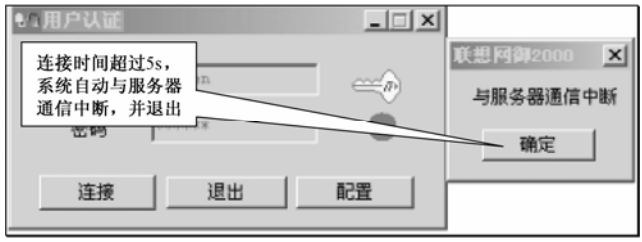


图 5.40　网络登录连接超时检查

⑥ 查看是否实现了设备特权用户的权限分离。登录防火墙查看“用户认证”情况，再通过本地服务器上的用户列表来查看具有不同权限的用户，从图 5.41 中可以看出对设备特权用户的权限分离情况。



图 5.41　特权用户权限分离检查

检查结论：该防火墙对边界和主要网络设备的管理员登录地址进行了限制；具有网络登录连接超时并自动退出功能；实现了设备特权用户的权限分离。符合检查要求。

最后需要提醒读者注意的是，在现场检查完成之后，测评人员应该填写“网络安全现场检查记录表”。其表格的相关格式可以参照前面几章，在此不再赘述。

5.2.3　网络安全测试

与网络安全现场检查工作相比较，网络安全测试工作也是属于“自选动作”，测评

人员应充分发挥自己的创造力来构思测试方案。第 3 级安全测评要求对网络安全的测试共有 6 类 9 项。

1．网络访问控制测试

第 3 级安全测评要求对网络安全的访问控制测试共有 2 项。

（1）测试边界网络设备，验证访问控制措施对未授权访问行为的控制是否有效。

测试目标：测试边界网络设备，可通过试图访问未授权的资源，验证访问控制措施对未授权的访问行为的控制是否有效。

测试对象：“天网”系统网络。

测试环境：目前业界使用的边界和主要网络设备有防火墙、边界网关、认证隔离设备、应用网关、路由器和三层交换设备六种。根据被测网络的具体结构和设备情况的不同，可以从上面列举的设备中选择对应的一种或几种设备来进行安全检查。在“天网”大型信息系统中使用的是防火墙。

测试方案：

技术路线

用外网未经授权的用户来对系统内网终端进行通信，如可以以未经授权的用户身份向内网某终端发送 ICMP 请求，查看防火墙是否对其进行阻止。如果成功阻止，说明系统对未授权通信行为的控制是有效的。

测试步骤

① 以管理员身份登录防火墙，查看防火墙策略，图 5.42 中的“permit”和“deny”分别代表了允许内网向外发送 ICMP 协议包和禁止内网向外网发送 ICMP 协议包的情况。



图 5.42　防火墙访问控制策略配置测试（1）

防火墙允许内网 192.168.0.0/24 对外网 192.168.1.0/24 发送 ICMP 协议包，如图 5.43 所示。

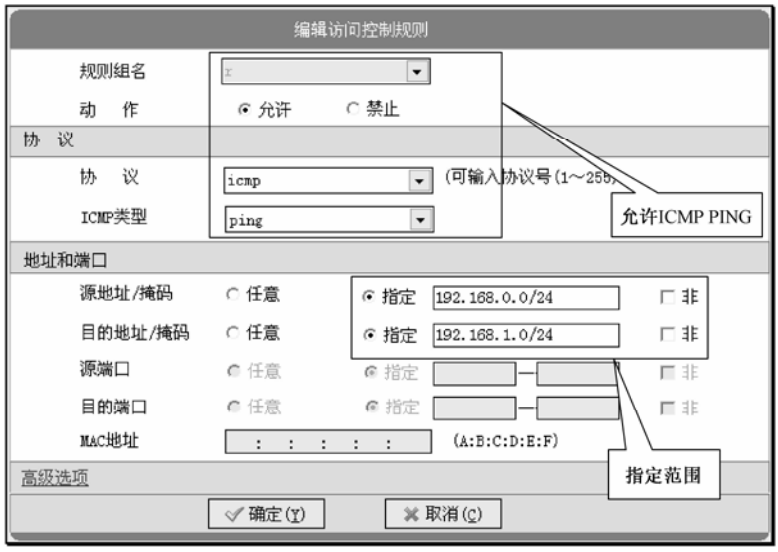


图 5.43　防火墙访问控制策略配置测试（2）

防火墙禁止外网 192.168.1.0/24 向内网 192.168.0.0/24 发送 ICMP 协议包，如图 5.44 所示。

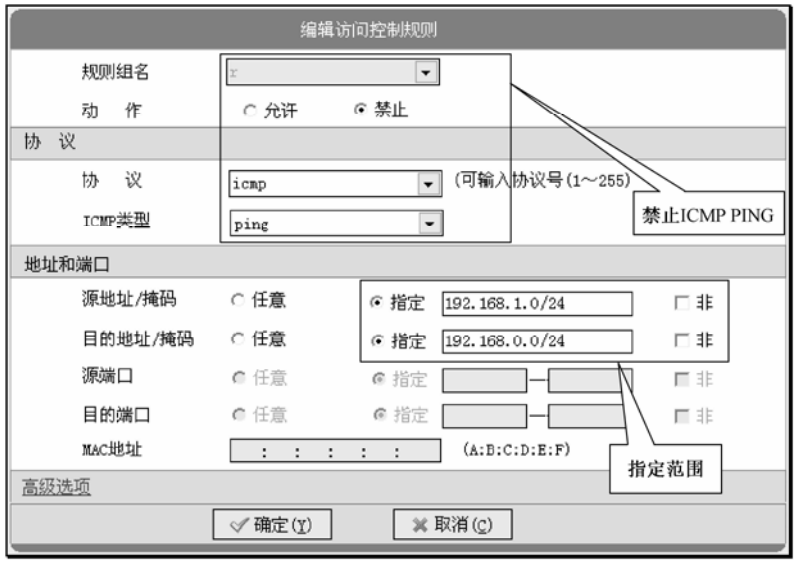


图 5.44　防火墙访问控制策略配置测试（3）

② 使外网终端 192.168.3.3 与内网终端 192.168.0.8 相互进行访问，网络拓扑图如图 5.45 所示。

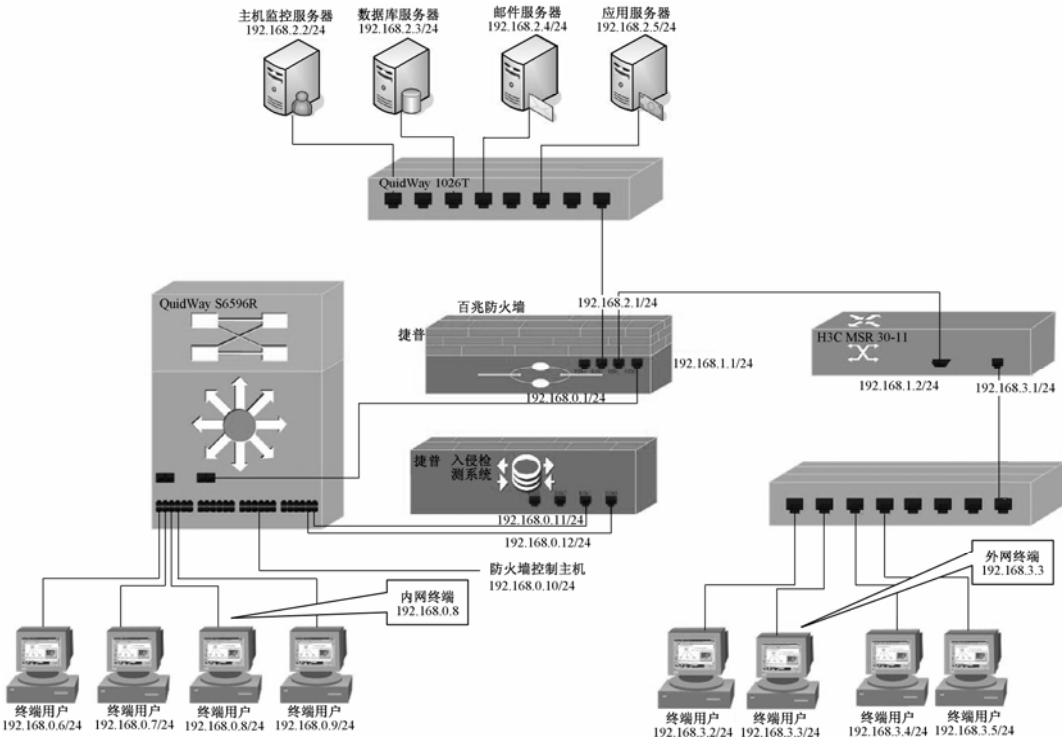


图 5.45　分别位于内、外网的两台终端拓扑示意图

内网终端向外网终端发送 ICMP 协议包成功，如图 5.46 所示。

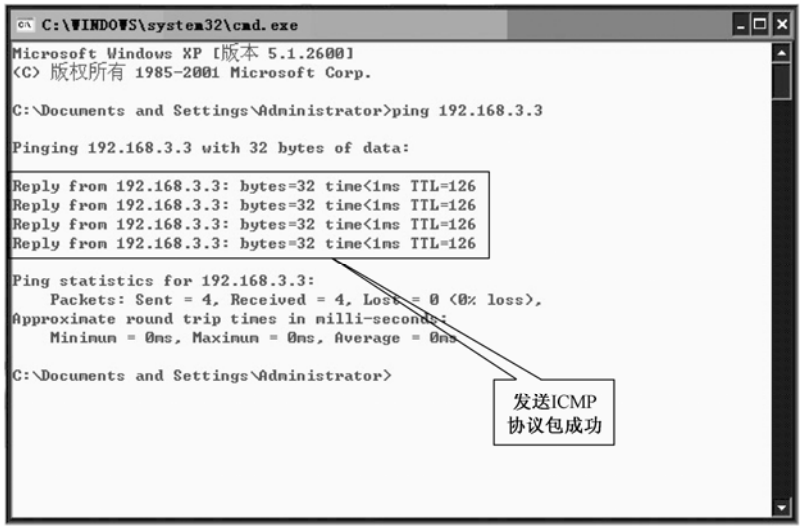


图 5.46　防火墙访问控制策略配置测试（4）

外网终端向内网终端发送 ICMP 协议包失败，如图 5.47 所示。

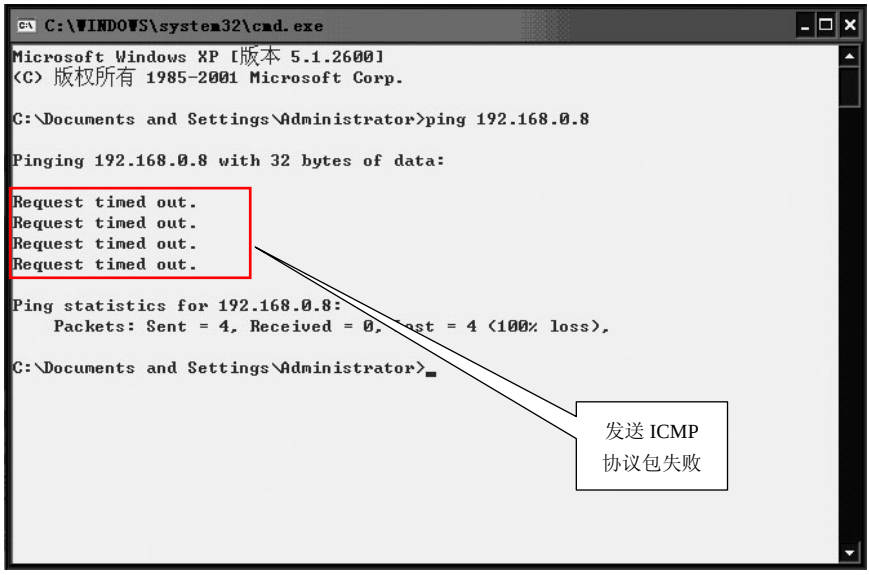


图 5.47　防火墙访问控制策略配置测试（5）

测试结论：该测试表明，外网非授权用户对内网进行访问时，访问被拒绝，所以访问控制措施是有效的，符合测试要求。

（2）对网络访问控制措施进行渗透测试，可通过采用多种渗透测试技术，验证网络访问控制措施不存在明显的弱点。

测试目标：采用渗透测试技术检查网络访问控制措施是否存在明显的弱点。

测试对象：“天网”系统网络。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

在外网采用渗透技术对内网进行测试时，查看防火墙是否对其进行阻止。如果成功阻止，说明网络访问控制措施是有效的，反之则说明网络访问控制措施存在弱点。下面的实验方案是预设一个具有“反弹端口”的木马程序（相当于为外网渗透攻击打开一个窗口），然后利用这个端口进行一系列的操作，如操作被攻击内网某终端上的文件、注册表和进程，甚至操作该终端的实时截屏等功能。

测试步骤

① 在内网某台终端上运行一个“反弹端口”程序。

② 在外网终端上启动“反弹端口”程序的客户端，找到内网中安装程序的终端，如图 5.48 所示。

③ 运行“反弹端口”程序，调阅内网终端文件，如图 5.49 所示。

④ 运行“反弹端口”程序的内网终端注册表，如图 5.50 所示。



图 5.48　反弹木马启动

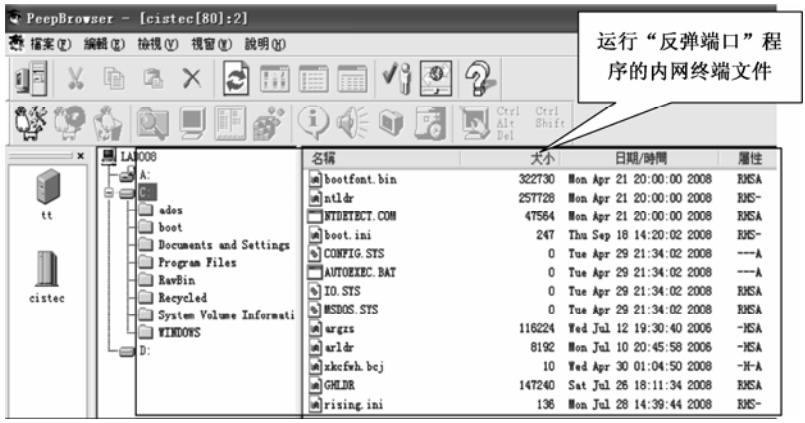


图 5.49　通过外网操纵内网终端反弹木马（1）

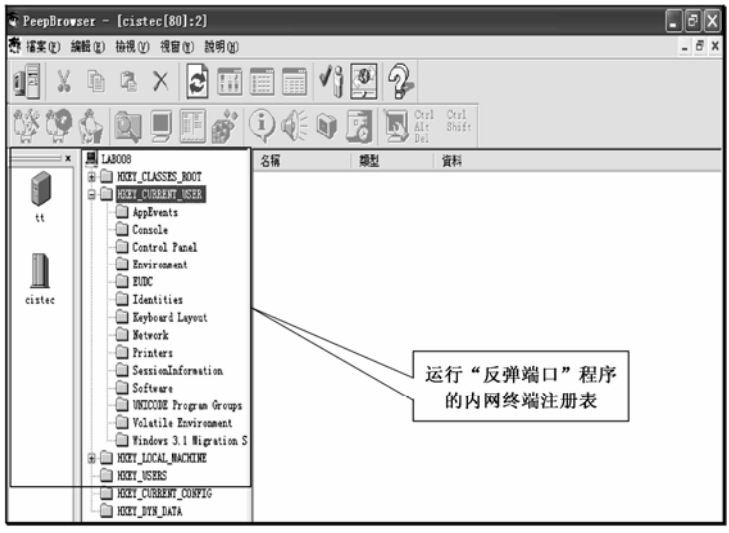


图 5.50　通过外网操纵内网终端反弹木马（2）

⑤ 运行“反弹端口”程序的内网终端进程，如图 5.51 所示。

⑥ 运行“反弹端口”程序的内网终端实时屏幕功能，如图 5.52 所示。

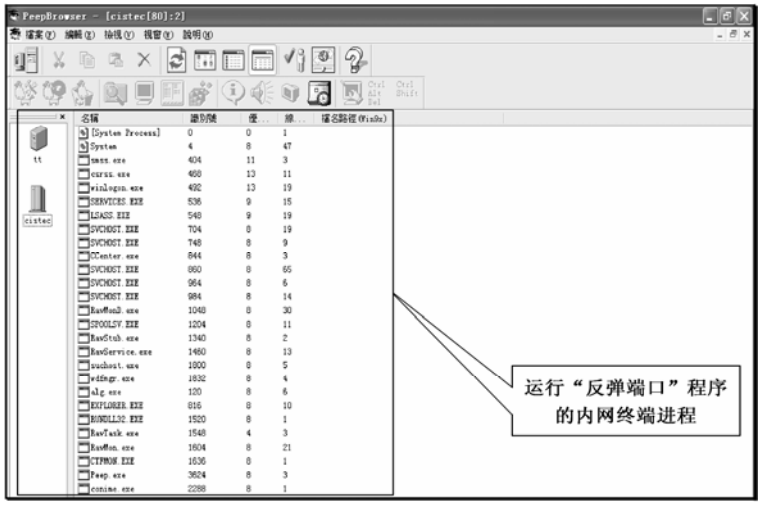


图 5.51　通过外网操纵内网终端反弹木马（3）

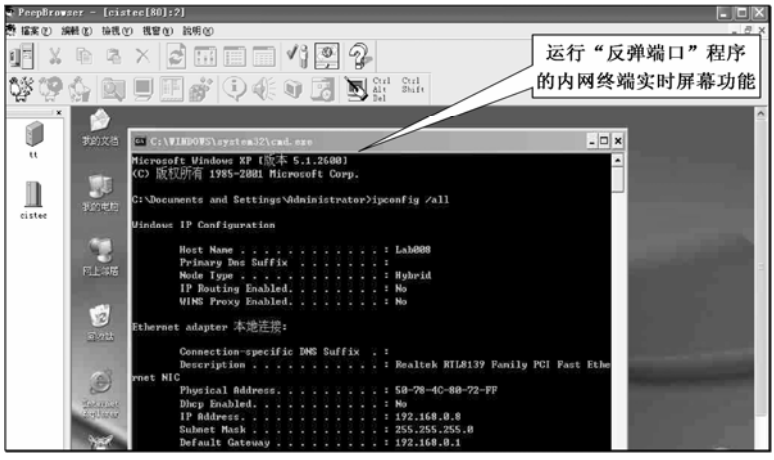


图 5.52　通过外网操纵内网终端反弹木马（4）

检查结论：该测试表明，在内网终端运行“反弹端口”程序的情况下，外网客户端可以通过“反弹端口”程序绕过防火墙进入内网，访问控制措施存在明显弱点，不满足检查要求。需要向读者指出的是，这个实验的前提是进行了具有特殊功能（反弹端口）的木马预置，然后再通过这个端口对内网终端进行全面控制和操作。因此，如果内网的病毒防护系统能够有效发挥作用，这个反弹端口木马是起不了作用的。由此可见，信息系统的防御体系应当是多种技术和设备协同工作才能够真正建立起来的。

2．拨号访问控制测试

第 3 级安全测评要求对网络安全的拨号访问控制测试只有 1 项。

测试边界网络设备，可通过试图非授权的访问，验证拨号访问措施能否有效对系统资源实现允许或拒绝用户访问的控制。

测试目的：验证通过拨号的网络用户对系统资源的使用和控制情况。

测试对象：“天网”系统网络。

测试环境：使用防火墙进行测试。

测试方案：

技术路线

客户端由 PPTP 拨号接入 VPN 网络，通过授权用户 test 和非授权用户 guest 分别对服务器进行访问。

测试步骤

① 用 test 账户登录 VPN 网络，然后查看登录状态，分别如图 5.53 和图 5.54 所示。



图 5.53　防火墙 VPN 登录测试



图 5.54　VPN 网络客户端 IP 地址分配测试

授权用户 test 通过 TCP/IP 登录服务器。VPN 网络为客户端（客户端 IP 为 192.168.3.3）分配一个虚拟网络 IP 地址为 192.168.0.2，服务器主机的 IP 地址为 192.168.1.100，此时若显示系统的连接状态正常，即表示客户端可以正常访问服务器。

② 用 guest 账户登录，因为 guest 账户为非授权用户，所以无法登录，其过程显示分别如图 5.55 和图 5.56 所示。

测试结论：通过以上测试表明，只有授权用户才可以访问系统资源。并且授权用户的权限是根据定制的策略决定的，非



图 5.55　非授权用户登录测试（1）

授权用户无法访问系统资源，因此满足检查要求。

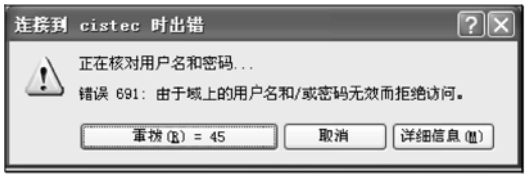


图 5.56　非授权用户登录测试（2）

3．网络安全审计测试

第 3 级安全测评要求对网络安全的网络安全审计测试只有 1 项。

测试边界和主要网络设备，验证安全审计的保护情况与要求是否一致。

测试目标：测试边界和主要网络设备，验证安全审计的保护情况与要求是否一致。

测试对象：“天网”系统网络。

测试环境：使用防火墙进行测试。

测试方案：

技术路线

用操作系统的普通用户来对日志进行修改，查看操作系统是否对其进行阻止，从而验证安全审计的保护情况。

测试步骤

用操作系统的普通账户来登录系统，并删除系统的审计日志记录。其运行结果如图 5.57 所示。

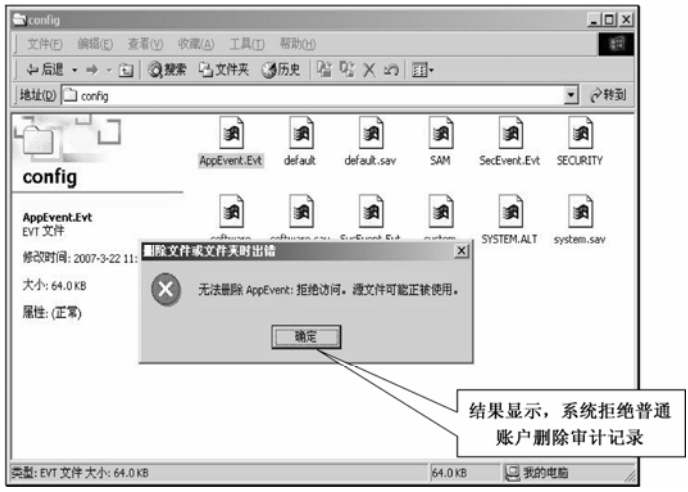


图 5.57　普通用户删除审计记录的测试

测试结论：该测试表明，用非授权用户删除审计记录将被系统拒绝，因此符合测试要求。

4．边界完整性检查测试

第 3 级安全测评要求对网络安全的拨号访问控制测试共有 2 项。

（1）测试边界完整性检查设备，是否能够确定出非法外连设备的位置，并对其进行有效阻断（如产生非法外连的动作，需查看边界完整性检查设备是否能够准确定位并进行阻断）。

测试目标：测试边界完整性检查设备，是否能够确定出非法外连设备的位置，并对其进行有效阻断。

测试对象：“天网”系统网络。

测试环境：使用防火墙进行测试。

测试方案：

技术路线

尝试从模拟内网向模拟外网（如 Internet）连接，并使用防火墙进行监控。一旦发现有非法外连现象，检查系统可否进行阻断。

测试步骤

用内网的 PC 客户端登录到外网的 Web 服务功能。从防火墙的监视会话栏中观察是否实时显示了此连接，并且查看是否可以手动断开此次会话，如图 5.58 所示。

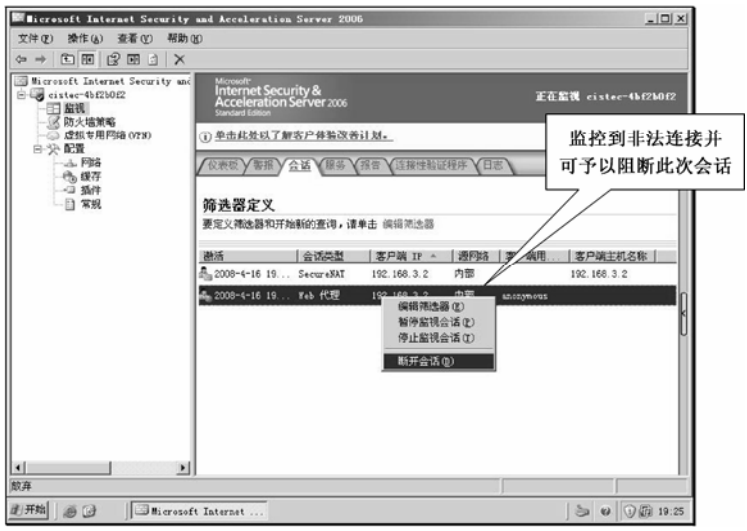


图 5.58　对非法外连的阻断测试

测试结论：该防火墙能确定出非法外连设备的位置，并对其进行了有效阻断。符合测试要求。

（2）测试边界完整性检查设备，是否能够对非授权设备私自连接到网络的行为进行检查，并准确定出位置，对其进行有效阻断。

测试目标：测试边界完整性检查设备，是否能够对非授权设备私自连接到网络的行

为进行检查，并准确定出位置，对其进行有效阻断。

测试对象：“天网”系统网络。

测试环境：操作系统自带路由功能模块。

测试方案：

技术路线

可以利用操作系统自带的路由功能来模拟测试。该路由功能对已建立的每一个连接都有实时的记录。如果产生非法接入的动作，可查看测试边界完整性检查设备是否能及时准确发现和确定出位置，并对其进行阻断。

测试步骤

通过模拟的专用 IP 地址 192.168.3.2 私自连接来访 IP 地址 192.168.2.1，此时系统界面如图 5.59 所示，从中可以看出，边界完整性检查设备可以准确对其定位。

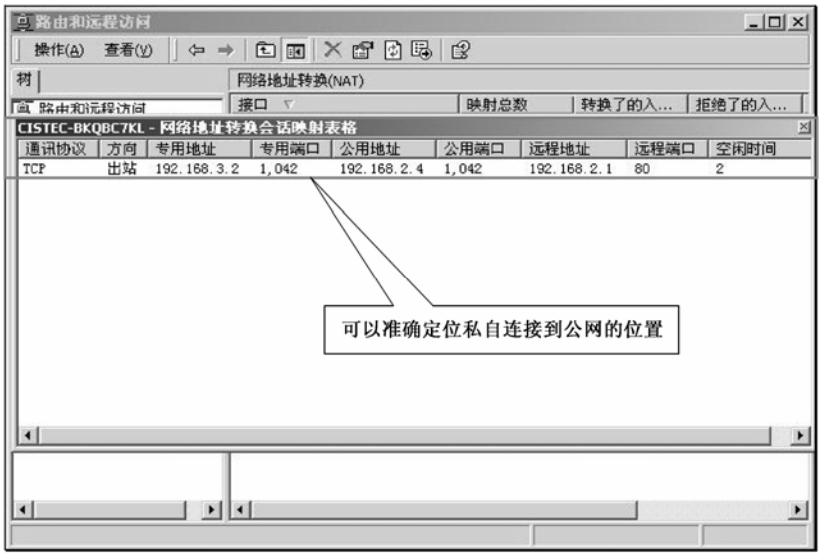


图 5.59　对私自外连的定位测试

测试结论：该测试表明，路由器对非授权设备私自连接到网络的行为能够进行实时跟踪，并准确定出位置，但不能进行阻断。因此该项检查只是部分符合测试要求。

5．网络入侵防范测试

第 3 级安全测评要求对网络安全的网络入侵防范测试共有 2 项。

（1）测试网络入侵防范设备，验证其监控策略是否有效。

测试目标：测试网络入侵防范设备，验证其监控策略是否有效。

测试对象：“天网”系统网络。

测试环境：使用防火墙进行测试。

测试方案：

技术路线

本测试的基本思想是模拟产生攻击动作，查看网络入侵防范设备的反应。具体的方案设想是使用“瑞星个人防火墙”（考虑到方便读者练习）来完成这个实验。首先，对目标主机进行 ping 攻击，然后查看防火墙是否对其进行了阻止，并且记录在相关的日志当中。

测试步骤

对装有入侵防范设备（防火墙）的主机发送“ping”指令，查看其日志，可以清楚地看到操作的时间、动作、方向和使用的协议，如图 5.60 所示。



图 5.60　防火墙监控策略测试

测试结论：该测试表明，防火墙配置的监控策略是有效的，因此符合测试要求。

（2）测试网络入侵防范设备，验证其报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警）。

测试目标：测试网络入侵防范设备，验证其报警策略是否有效。

测试对象：“天网”系统网络。

测试环境：使用防火墙进行测试。

测试方案：

技术路线

继续前一个实验，对目标主机进行 ping 攻击，查看目标机上的杀毒软件是否可以对这个攻击行为进行实时报警。

测试步骤

① 打开“运行”窗口，对装有入侵防范设备的目标网络中的一台主机不停地发送

“ping”命令。

② 查看被发送“ping”命令的那台主机，从界面可以发现在屏幕右下方有报警标志。为了验证这个报警策略的有效性，可以通过查看日志来判断，如图 5.61 所示。



图 5.61　对 ping 攻击行为进行报警测试

测试结论：该防火墙配置的报警策略有效，符合测试要求。

6．网络设备防护测试

第 3 级安全测评要求对网络安全的网络设备防护测试只有 1 项。

通过使用各种渗透测试技术（如口令猜解等）对边界和主要网络设备进行渗透测试，以验证网络设备的防护能力是否符合要求。

该渗透测试案例与本书第 4 章所使用的技术手段类似，留给读者进行练习。

请读者注意，国家第 3 级安全标准对“结构安全和网段划分”和“恶意代码防范”没有测试要求。

至此，我们已完成了对网络安全的测评。读者应该对本章所涉及的“问卷调查”、“现场检查”和测试这三部分的记录进行分析，并整理成“天网系统网络安全测试技术报告”。

5.3　本章小结

- 网络安全测评的三种主要方法
- 结构安全与网段划分测评
- 网络访问控制测评
- 拨号访问控制测评

- 网络安全审计测评
- 边界完整性检查测评
- 网络入侵防范测评
- 恶意代码防范测评
- 网络设备防护测评

尾声：墙、门、界

荷兰伦伯朗价值连城的名作，从不失手的传奇绅士大盗，极度震惊又悲愤的保险公司，美艳的诱捕陷阱，全球防卫最森严的银行，千禧虫蠢蠢欲动的千禧年除夕夜，穿墙透壁的阴影，红外线光辉交织中轻柔的舞姿……

这是《偷天陷阱》中的一幕幕景象。在“大盗”面前，墙怎么了？门怎么了？界又在何处？

这在网络世界里，只是有过之而无不及。

在网络世界里，墙是什么？门又如何？界在哪里？

在网络世界里，与其说墙，不如说门。比如防火墙，它的作用更像一道门，一道有卫兵把守的门，它知道谁可以进，谁可以出，谁不能进出。如果是一堵墙的话，那就是任何人都不能进出了。

界在哪里？虚拟空间的界，不是用地图就可以直观地标明的，网络边界比地域的边界复杂得多，它包括:

组织机构网络（无论广域网还是局域网）与 Internet 的边界;

组织机构网络与合作伙伴的互联边界;

组织机构内部网（Intranet）中不同安全域间的边界。

还有:

组织机构网络与电信专用网的边界;

组织机构网络与传统电话网的边界;

组织机构网络与无线网的边界; 等等。

新的首都博物馆美轮美奂，更让人惊羡的是其安全保障体系：双层的、必经布满监控的环形走廊才能进入内层的建筑结构，被动式（无须发出探测信号）红外探测……使得“大盗”妄图“穿墙透壁”无异于自投罗网，《偷天陷阱》中那轻曼的舞蹈也无法在此再现（据央视 10 频道——探索 • 发现节目）。

应该让我们的网络空间也达到如此境界，这需要我们的智慧。

观感

（1）网络安全测评与主机安全测评有什么相同之处和不同之处？

（2）请完成本章“网络设备防护测试”，并出具测试报告。

Snort 是一套免费的入侵检测软件工具，请读者在网上下载之后完成以下有关入侵检测设备的现场检查工作，并出具检查报告:

① 检查网络入侵防范设备，查看是否能检测端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为。

② 检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源 IP、攻击的类型、攻击的目的和攻击的时间等信息。

③ 检查网络入侵防范设备，查看其规则库是否为最新。

（3）请将本章“现场检查”和测试两部分的记录进行分析和整理，并出具“天网”系统网络安全测试技术报告。

第 6 章
应用安全测评技术





中国古代地震仪

谨以此奖授予那些在计算机领域做出重大原创性贡献的人。

——A.M.Turing Award 颁奖原则

序幕：“机器会思考吗？”

“他活着的时候受尽屈辱。今天，让我们恢复他应有的荣誉，以赎清我们整个国民的羞耻吧”。1998 年 6 月 23 日，在阿兰·图灵（Alan M.Turing）愤然辞世 44 年之后，英国各界人士聚集在伦敦“柱廊”酒店——图灵的诞生地，纪念这位伟大的科学家 86 岁诞辰。英国政府文体大臣首次代表英国政府和国民在纪念集会上向这位“天下人负他，他却未负天下人”的科学巨匠，为世界反法西斯战争做出卓越贡献的战士道歉。

“机器会思考吗？”1950 年，时年 38 岁的图灵发表了这篇划时代的论文，奠定了现代人工智能的基础。4 年后，当他抵抗不住世俗的偏见吞下毒苹果的那一刻，是否会想到今天的人们在尽情享受计算机应用的时候对他的缅怀之情呢？

尽管我们至今还不知道该怎样回答图灵的这个问题，然而我们“尴尬”地发现由于计算机无所不在，整个人类社会的发展乃至人的思维习惯却正在受到这些“机器”的影响。这也许是图灵先生始料不及的吧。所以本章的目的就是与读者一道去探讨怎样测评计算机应用系统的安全性。

要点：本章结束之后，读者应当了解和掌握

- 应用安全测评有几个环节？
- 国家标准对应用安全测评有何要求？
- 怎样进行应用安全测评？

6.1 应用安全测评的诸方面

在前面各章已经对“信息高速公路”建设的基础设施——数据、主机和网络的安全测评进行了介绍之后，接下来自然就要考虑在这条“高速公路”上行驶的各种“车辆和人员”，也就是应用系统的安全了。



目前国内外对应用安全的研究目光已经转向了所谓的“可信软件”。可信软件属性包括了“软件安全性”、“软件可靠性/容错性”、“软件可生存性”等方面。在这些属性中，软件可靠性/容错性的研究历史较长，结果也相对丰富。然而什么是软件安全性？它与信息安全是什么关系？我们可以用类似于平均故障时间那样的概念来定量刻画软件安全性吗？软件保密性是什么意思？美国自然科学基金会最近又提出了所谓的 cybertrust……

正如在本章序幕中所描述的那样，由于人们给计算机（网络）注入了软件的灵魂，所以现在计算机系统远远不只是为了某个科学问题而进行计算，还被应用到了人类工作和生活的方方面面。那么，为了考虑计算机应用系统的安全，需要逐一分析各行各业的应用特点吗？当然应该。然而您能告诉我们人类社会有多少种行业吗？这些行业中使用计算机的芸芸众生有些什么样的行为习惯吗？非常遗憾，这是很难做到的。因此我们只能把握计算机系统的应用基础有些什么样的安全测评要求，以便在这条“高速公路”上行驶的“人员”能够“放心驾驶”。至于“他们开什么样的车，开往何方”等，则只好在今后的测评工作中就事论事了，读者可以在下面对“天网”应用系统的案例分析中窥其一斑。

在介绍应用安全测评要求之前，再次建议读者回忆一下前面各章的测评环节，以便比较其中的异同。国家有关标准对应用安全的测评依然采用“访谈、检查和测评”三种手段。应用安全的测评条款分为“身份鉴别”、“访问控制”、“安全审计”、“剩余信息保护”、“通信完整性”、“通信保密性”、“抗抵赖”、“软件容错”和“资源控制”9 个环节。记忆力好的读者可能已经发现了这些条款中有几项是新出现的名词。下面分别进行介绍。

（1）身份鉴别。与第 4 章“主机安全测评”的身份鉴别不同，这里的身份鉴别专指软、硬件应用系统应该具有身份鉴别功能。换言之，即使您成功地登录了主机，如果要使用某种应用软件，也必须通过身份鉴别。

（2）访问控制。应用系统应该具备自主访问控制功能。

（3）安全审计。应用系统应该具备安全审计功能。

（4）剩余信息保护。与主机安全测评原理类似，但针对的是应用系统。

（5）通信完整性。与“数据完整性测评”原理类似，但强调的是应用系统。

（6）通信保密性。与“数据保密性测评”原理类似，但测评的是应用系统。

（7）抗抵赖。这是一个新的测评项。在法制社会中人类的“契约”活动是由具有法律效力的合同等“证据”来保障的。在虚拟空间中一样需要这种保障机制。

（8）软件容错。这也是一个新的测评项。“容错”是“防错”的手段之一。它要求应用软件系统具有较强的健壮性。

（9）资源控制。与“主机安全测评”类似，但对象是应用系统。

应用安全测评就是对上面 9 个环节，利用访谈、检查和测评等手段进行分析。图 6.1 所示为应用安全测评的框架图。

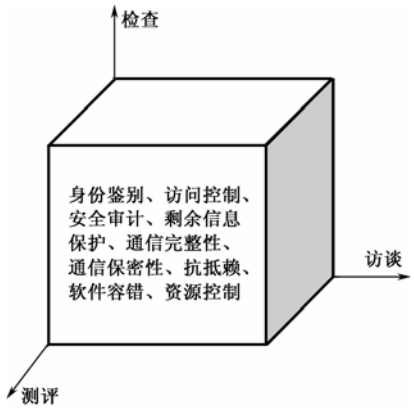


图 6.1　应用安全测评的框架图

6.2　应用安全测评的实施

现在进入信息系统应用安全的测评环节。为此需要开始以下工作。

6.2.1　应用安全访谈调研

与前面进行的访谈调研略有不同的是，这次的访谈对象不仅包括信息系统的各级管理和技术人员，还包括应用系统的使用人员和开发商，访谈一共 9 项。在该环节结束的时候，也是用一个访谈调研问卷表来总结和细化各个访谈项的。

1．身份鉴别访谈

第 3 级安全测评要求对应用安全的身份鉴别访谈共有 2 项。

（1）应访谈应用系统管理员，询问应用系统是否采取身份标志和鉴别措施，具体措施有哪些？系统采取何种措施防止身份鉴别信息被冒用（如具有复杂性，指采用混合有大、小写字母、数字和特殊字符，以及口令周期等）。

（2）应访谈应用系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的？

2．访问控制访谈

第 3 级安全测评要求对应用安全的访问控制访谈只有 1 项。

应访谈应用系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些？自主访问控制的粒度如何？

3．安全审计访谈

第 3 级安全测评要求对应用安全的安全审计访谈只有 1 项。

应访谈安全审计员，询问应用系统是否有安全审计功能，对事件进行审计的选择要求和策略是什么？对审计日志的保护措施有哪些？

4．剩余信息保护访谈

第 3 级安全测评要求对应用安全的剩余信息保护访谈只有 1 项。

应访谈应用系统管理员，询问系统是否采取措施保证对存储介质中的残余信息进行删除（无论这些信息是存放在硬盘上还是在内存中），具体措施有哪些？

5．通信完整性访谈

第 3 级安全测评要求对应用安全的通信完整性访谈只有 1 项。

应访谈安全管理员，询问业务系统是否在传输过程中有数据进行完整性保护的操作，具体措施是什么？

6．通信保密性访谈

第 3 级安全测评要求对应用安全的通信保密性访谈只有 1 项。

应访谈安全管理员，询问业务系统数据在通信过程中是否采取保密措施（如在通信双方建立连接之前利用密码技术进行会话初始化验证，在通信过程中对整个报文或会话过程进行加密等），具体措施有哪些？

7．抗抵赖访谈

第 3 级安全测评要求对应用安全的抗抵赖访谈只有 1 项。

应访谈安全管理员，询问系统是否具有抗抵赖的措施，具体措施有哪些？

8．软件容错访谈

第 3 级安全测评要求对应用安全的软件容错访谈只有 1 项。

应访谈应用系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对通过人–机接口输入或通过通信接口输入的数据进行有效性检验等），具体措施有哪些？

9．资源控制访谈

第 3 级安全测评要求对应用安全的资源控制访谈只有 1 项。

应访谈应用系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制，对一个时间段内可能的并发会话连接数进行限制，对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额等），具体措施有哪些？

问卷调查表设计

通过前几章的介绍，想必读者对问卷调查表的设计已经不再感到陌生了。在应用安全访谈工作中，依然是将“身份鉴别”、“访问控制”、“安全审计”、“剩余信息保护”、“通信完整性”、“通信保密性”、“抗抵赖”、“软件容错”和“资源控制”9 项访谈内容作为问卷调查表的第 1 列，然后针对各种应用系统（如 OA 系统、财务系统和邮件系统等）进行细化分类。

在进行“身份鉴别”访谈的时候，关注的重点是应用系统是否具备身份鉴别功能。同理，“访问控制”和“安全审计”类别的访谈也是重点关注应用系统、应用软件。

在进行“剩余信息保护”访谈的时候，关注的重点还包括各种移动存储介质等。

在进行“通信完整性”和“通信保密性”访谈的时候，更多的是在应用层上关注是否满足完整性和保密性要求。

在进行“抗抵赖”访谈的时候，由于现在大量的应用软件已经可以使用电子签章等技术（如中国不少电子政务办公系统中的公文流转就采用了电子签章，中国颁布的《电子签章法》也对电子商务领域使用数字证书进行了规范），所以这应当是访谈的重点之一。

在进行“软件容错”访谈的时候，关注的是应用软件是否具有“回退处理”和数据恢复等项功能。这里需要向读者指出的是，由于软件容错的各种技术指标已经相对成熟和稳定，国家也颁布了有关软件容错性方面的系列标准，所以有兴趣的读者可以在国家有关软件容错、软件可靠性等标准的基础上来细化这个问卷调查表。

在进行“资源控制”访谈的时候，关注的是各种应用软件（系统）是否能够对会话数进行限制以及用户对资源的占有情况等。

表 6.1 是应用安全访谈调研表模板，仅供读者参考。

表 6.1　应用安全访谈调研表模板

访谈类型	设 备 型 号	访 谈 内 容	访 谈 对 象	备注
身份鉴别	应用系统类型 ☐ OA 系统 ☐ 财务系统 ☐ 邮件系统 ☐ 审计系统 ☐ 其他特定应用系统（请注明） 数据库 ☐ Oracle ☐ SQL ☐ 其他	身份标识和鉴别 ☐ 身份标识和鉴别措施（具体措施） ☐ 身份鉴别信息被冒用（如何防止） 用户标识是否唯一 ☐ 是　☐ 否 是否有登录失败处理措施 ☐ 是　☐ 否 （具体措施） 数据库身份标识与鉴别机制 ☐ 口令（口令设置策略） ☐ 登录失败处理（处理措施） 用户标识是否唯一 ☐ 是　☐ 否 ☐ 其他	☐ 系统管理员 ☐ 安全检查员 ☐ 安全审计员 ☐ 数据库管理员	
访问控制		是否启用访问控制措施 ☐ 是　☐ 否 ☐ 自主访问控制是否设置有控制粒度 ☐ 是否授权主体设置对系统功能操作和对数据访问的权限 ☐ 是否实现了应用系统特权用户的权限分离 ☐ 权限分离是否用最小授权原则 具体访问控制措施 自主访问控制粒度	☐ 系统管理员 ☐ 安全检查员 ☐ 安全审计员 ☐ 数据库管理员	

续表

访谈类型	设 备 型 号	访 谈 内 容	访 谈 对 象	备注
安全审计		应用系统是否具有安全审计功能 □ 是　□ 否 □ 应用系统安全审计是否覆盖到每个用户 □ 安全审计是否记录系统重要的安全事件 □ 安全事件的记录是否包括时间、类型、主体标识、客体标识和事件结果 □ 安全审计能否生成审计报表 □ 安全事件能否提供指定事件的实时报警功能 □ 审计记录是否受到保护 审计事件的选择要求和策略	□ 系统管理员 □ 安全检查员 □ 安全审计员 □ 数据库管理员	
剩余信息保护		是否对存储介质中残余信息采取处理措施 □ 是　□ 否 □ 是否保证用户信息在被释放或分配给其他用户前得到完全清除 □ 是否确保系统内的文件、目录和数据库记录在被释放或分配给其他用户之前得到完全清除 具体措施	□ 系统管理员 □ 安全检查员 □ 安全审计员 □ 数据库管理员	
通信完整性		是否对系统数据在传输过程中采取保证完整性的措施 □ 是　□ 否 □ 通信双方是否约定密码算法计算报文验证码 □ 通信双方在通信过程中根据校验码判断对方报文的有效性 具体措施	□ 系统管理员 □ 安全检查员 □ 安全审计员 □ 数据库管理员	
通信保密性		是否能在系统通信过程中提供保证数据保密性的措施 □ 是　□ 否 □ 通信双方建立连接之前用密码技术进行会话验证 □ 通信过程中对敏感信息进行加密 □ 是否具有符合国家有关部门要求或国家标准要求的密码算法 具体措施	□ 系统管理员 □ 安全检查员 □ 安全审计员 □ 数据库管理员	

续表

访谈类型	设 备 型 号	访 谈 内 容	访 谈 对 象	备注
抗抵赖		系统是否具有抗抵赖的措施 □ 是　□ 否 □ 应用系统是否采用数字签名技术 □ 应用系统在通信中能否为数据原发者或接收者提供数据原发证据的功能 □ 应用系统在通信中能否为数据原发者或接收者提供数据接收证据的功能 具体措施	□ 系统管理员 □ 安全检查员 □ 安全审计员 □ 数据库管理员	
软件容错		业务系统软件容错的措施 □ 通过人–机接口输入或通过通信接口输入的数据进行有效性检验 □ 是否对自身错误的作用具有屏蔽作用 □ 应用系统是否可以从错误状态恢复到正常状态 □ 应用系统发生错误时，是否能完成预期的功能 □ 应用系统发生错误时，是否能实施必要的措施（数据保存） 具体措施	□ 系统管理员 □ 安全检查员 □ 安全审计员 □ 数据库管理员	
资源控制		业务系统资源控制的措施 □ 是否对应用系统的最大并发会话连接数进行了限制 □ 是否禁止同一用户在同一时间并发登录 □ 是否对一个时间段内可能的并发会话连接数进行了限制 □ 是否对一个用户或一个进程占用的资源分配了最大限额和最小限额 具体措施	□ 系统管理员 □ 安全检查员 □ 安全审计员 □ 数据库管理员	
被测评机构下属部门		部门主管姓名		访谈
测评机构下属部门		测评人员姓名		日期

6.2.2　应用安全现场检查

应用安全现场检查过程主要是测评工程师对各种应用系统（主要是软件系统）及其相关文档资料进行检查。毫无疑问，一个复杂的信息系统上面运行了多种应用软件。因此，国家标准在这方面强调的是对“主要的应用系统”进行检查。考虑到便于读者进行练习，下面以“天网”系统的内部办公邮件系统 Exchange Server 2003 为例，向读者介

绍应用安全现场检查的主要工作。

1．身份鉴别现场检查

第 3 级安全测评要求对应用安全的身份鉴别检查共有 5 项。

（1）检查设计/验收文档，查看文档中是否有系统采取了唯一标识（如用户名、UID 或其他属性）的说明。

（2）检查操作规程和操作记录，查看其是否有身份标识和鉴别的操作规程、审批记录和操作记录。

上述两项为文档现场检查，不再赘述。

（3）检查主要应用系统，查看其是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别。

检查目标：检查是否采用了两种及两种以上身份鉴别技术进行身份鉴别。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

在邮件服务器上，安装 Exchange Server 2003，按要求配置好 DNS 和 Exchange Server 2003 后，查看 Exchange Server 2003 是否可以设置检查要求中的第一和第二两种组合的验证方式来进行用户登录身份鉴别（如采用用户名/口令、智能卡、动态口令、数字证书和生物识别技术中的任意两个组合。本实验假设为口令与智能卡的组合）。

检查步骤

查看除用户口令登录的方式之外，是否还需要其他的用户登录身份鉴别机制，如图 6.2 所示。

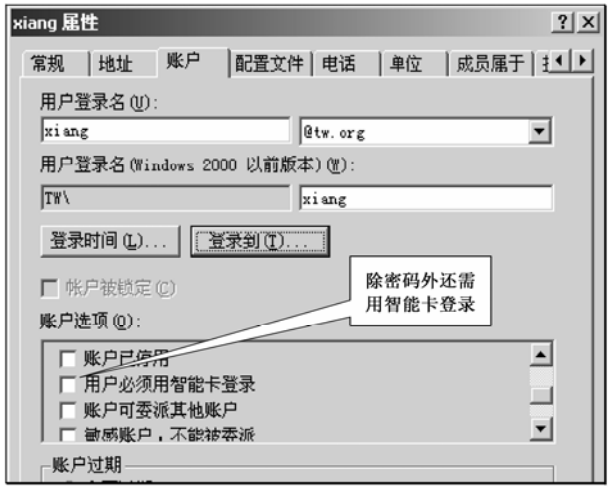


图 6.2　多因素身份鉴别检查

检测结论：由于除口令之外，还需智能卡才能登录，所以该邮件系统用户身份鉴别项符合检查要求。

（4）检查主要应用系统，查看其是否配备了身份标识和鉴别功能；查看其身份鉴别信息是否具有不易被冒用的特点，是否配备鉴别信息复杂度检查功能，以保证系统中不存在弱口令。

检查目标：检查主要应用系统，查看其是否配备了身份标识（如建立账号）和鉴别功能（如口令等）；查看其身份鉴别信息是否具有不易被冒用的特点，如具有复杂性（具有一定长度及是否采用了字母、数字和特殊字符相组合等）或为了便于记忆使用了令牌，是否配备鉴别信息复杂度检查功能，以保证系统中不存在弱口令。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

在上一个查看是否采用两个及两个以上身份鉴别技术的组合来进行身份鉴别的检查工作中，已经核实了“天网”邮件服务器具有两种以上的身份鉴别功能。现在继续深化其身份鉴别功能的检查。

在天网邮件子系统服务器上安装 Exchange Server 2003 后，按要求配置好 DNS 和 Exchange Server 2003，再在 AD 上创建新的账户。需要检查 Exchange Server 2003 这个应用系统对新建的用户是否能够按照上述要求进行粒度更细的身份鉴别。

先对新创建的用户口令进行初始化，按提示步骤进行操作，查看最后能否成功创建用户。在创建新的用户并初始化口令时，将口令初始化为“12”查看系统是否能及时对用户初始化的口令进行复杂度检查，以防止存在弱口令或假冒身份登录情况发生。

检查步骤

① 查看是否可以建立新账户。我们在 Exchange Server 2003 邮件服务器上建立了一个模拟“天网”（tw.org）系统的邮件系统，然后在这个目录下进行“新建/用户”的操作，如图 6.3 所示。

② 接下来查看系统对新用户是否具备最基本的身份鉴别功能，即新建用户密码的时候需要进行密码确认，如图 6.4 所示。

③ 现在检查 Exchange Server 2003 是否配备了鉴别信息复杂度的检查功能。在初始化用户口令时，我们故意使用简单的口令“12”，然后查看是否有口令复杂度检查功能。如图 6.5 所示，在输入了简单口令“12”之后，系统自动进入了“确认密码”的环节，说明没有口令复杂度检查的功能。

检查结论：该邮件系统用户身份标识和鉴别功能项符合检查要求，但鉴别信息复杂度检查项不符合要求。



图 6.3　新建一个用户



图 6.4　对新建用户配置口令



图 6.5　口令复杂度检查

（5）检查主要应用系统，查看其是否使用并配置了登录失败处理功能。

检查目标：检查主要应用系统是否使用并配置了登录失败处理功能。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

针对查看其是否使用并配置了登录失败处理功能的要求，可以考虑两种实验：一是按照常规方式，如登录失败次数超过设定值，系统自动退出的实验方式。这个实验与第5 章所介绍的方法类似（当然，请读者注意这里要检查的是应用软件系统 Exchange Server 2003），所以从略。二是查看 Exchange Server 2003 是否可以对每一用户登录的时间段进行设置，从而使得对这一项检查条款的检查粒度更细。

检查步骤

检查邮件服务器 Exchange Server 2003 对用户“xiang”登录时间段的设置情况，其中浅色代表“拒绝登录”的时间段，深色代表“允许登录”的时间段，如图 6.6 所示。

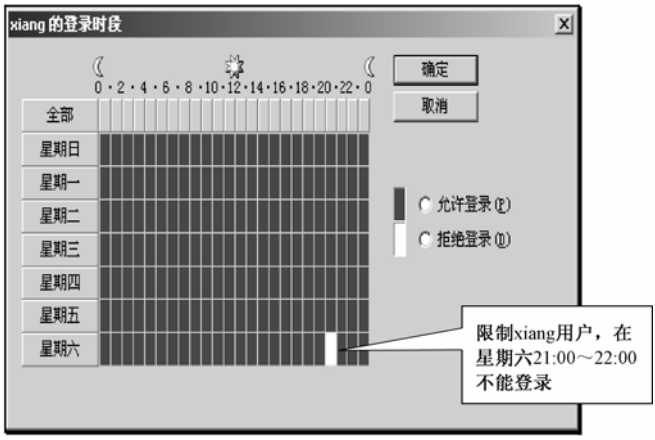


图 6.6　用户登录时间段设置检查

检查结论：该邮件系统登录失败处理符合检查要求。

2．访问控制现场检查

第 3 级安全测评要求对应用安全的访问控制检查共有 5 项。

（1）检查主要应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体（如文件和数据库中的数据）的访问。

检查目标：检查是否可对授权主体进行系统功能操作和对数据访问权限进行设置。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

由于我们现在检查的对象是邮件应用系统，所以访问控制机制就是针对邮件应用而言的。设计的访问控制检查方案有两个：一是查看邮件服务器是否可以限制每个用户发送/接收邮件的大小（从而也就间接地表明控制了用户对文件或数据的访问）；二是查看 Exchange Server 2003 能否对邮件来源进行控制。

检查步骤

检查邮件服务器 Exchange Server 2003 对用户传递邮件大小是否进行了设置，同时也查看是否能够对邮件来源进行控制，如图 6.7 所示。

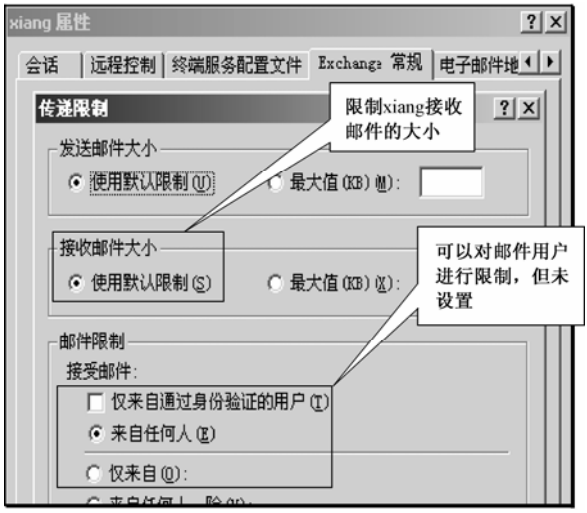


图 6.7　邮件服务器对用户及邮件大小进行限制的检查

检查结论：该邮件系统对数据访问权限进行了限制，符合检查要求。

（2）检查主要应用系统，查看其自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作。

检查目标：检查自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

初看起来这是一个比较晦涩的检查要求，什么是与信息安全直接相关的主体、客体及它们之间的操作？实际上很简单，这个检查设计方案是要查看 Exchange Server 2003 是否可以对每个授权用户（主体）设置用户传递（发送和接收）邮件（客体）的大小，

如果这一设置能对每个授权主体生效，则邮件应用系统的被检查项满足要求。

检查步骤

检查邮件服务器 Exchange Server 2003 是否能对用户“xiang”传递（发送或接收）邮件的大小进行设置，如图 6.8 所示。

检查结论：该邮件系统自主访问控制的覆盖范围符合要求。

需要指出的是，对该检查项的实验方案是多种多样的。所以建议读者根据自己的理解来进行该项的检查。

（3）检查主要应用系统，查看该系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能。

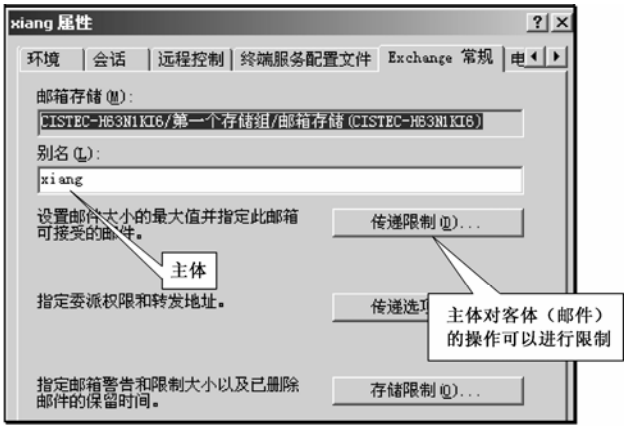


图 6.8　主、客体操作限制的检查

检查目标：检查应用系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

查看 Exchange Server 2003 是否对某一具体用户的操作权限进行了设置，如创建其他用户、传递（发送和接收）邮件（客体）的大小，如果能对每个授权主体（用户）设置操作权限，则邮件应用系统被检查项满足要求。

检查步骤

检查邮件服务器 Exchange Server 2003 是否能对用户传递（发送或接收）邮件大小进行设置，即对用户的操作权限进行设置，如图 6.9 所示。

检查结论：该邮件系统能对授权主体进行系统功能操作和对访问权限进行设置，符合检查要求。顺便指出，上一个实验中的邮件“传递限制”也可支持该项检查。

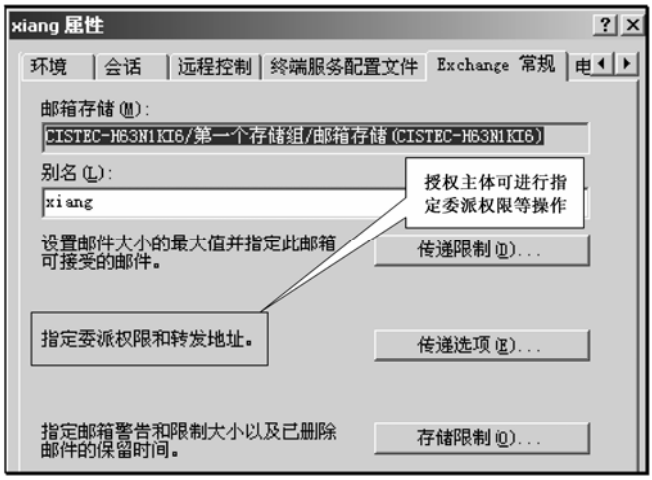


图 6.9　用户权限设置检查

（4）检查主要应用系统，查看其特权用户的权限是否分离（如将应用系统管理员、安全管理员和审计员的权限分离），是否按用户承担任务情况，只授予他们所需的最小权限，且权限之间是否相互制约（如应用系统管理员、安全管理员等不能对审计日志进行管理，而安全审计员不能管理涉及审计功能的开启、关闭和删除等重要事件的审计日志等）。

检查目标：检查其特权用户的权限是否分离。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

尽管在主机级、网络级均进行了用户权限分离的检查（见第 4、5 两章），但按照信息系统的第 3 级安全测评要求，在应用级上也需要进行用户权限分离的检查。在本案例中，设计的方案是查看 Exchange Server 2003 是否可以创建新的用户，这是最首要的条件，因为不同权限的用户不能是同一用户。在此基础上，再查看是否有 Administrator 和一般用户，查看管理员用户和普通用户权限设置的区别。如果根据不同角色对不同用户可以设置相应符合要求的权限，则邮件子系统被检查项满足要求。

检查步骤

① 先检查该邮件服务器 Exchange Server 2003 是否能创建多个用户（此步骤在本章身份鉴别现场检查（4）中已验证），然后查看针对 Administrator 设置不同权限的情况，如删除、读取、更改及是否取得完全权限等，如图 6.10 所示。

② 检查天网邮件服务器 Exchange Server 2003 是否能创建多个用户（此步骤在本章身份鉴别（4）中已验证），查看是否为普通用户“xiang”设置了不同的权限，如删除、读取、更改及是否取得完全权限等。如图 6.11 所示，普通用户 xiang 只有“读取权限”，没有其他权限。



图 6.10　特权用户权限分离检查（1）



图 6.11　特权用户权限分离检查（2）

检查结论：该邮件特权用户的权限分离设置项符合检查要求。

（5）检查主要应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用。

检查目标：检查应用系统是否有限制默认用户访问权限的功能。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

可以换位思考这个检查要求。例如，从 Exchange Server 2003 所管理的用户范围里，选择一个用户（默认）来进行访问验证。为此，在某个邮件子系统的客户端内安装好邮件客户端软件 Outlook，通过查看客户端软件 Outlook 是否可以将一个用户设置为默认登录用户来进行检查。如果可以设置，则说明邮件子系统此项不符合要求；否则符合要求。

检查步骤

检查天网邮件子系统内各个客户端软件 Outlook，是否可以将一个用户设置成为默认登录用户，如图 6.12 所示。

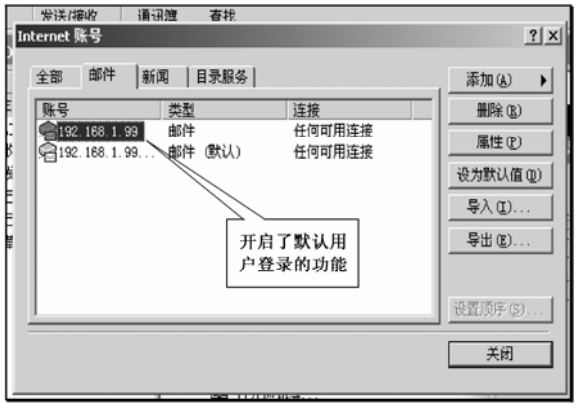


图 6.12　默认用户登录限制检查

检查结论：该邮件系统不能限制默认用户访问权限，因此邮件系统的功能设置不符合检查要求。

3．安全审计现场检查

第 3 级安全测评要求对应用安全的安全审计检查共有 5 项。

（1）检查主要应用系统，查看其当前审计范围是否覆盖到每个用户。

检查目标：检查主要应用系统当前审计范围是否覆盖到每个用户。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

这个检查要求非常明确，只需查看邮件服务器 Exchange Server 2003 是否可以启用针对每一个用户的安全审计日志，如果可以启用，则说明审计日志记录了当前所有用户

的行为，邮件应用系统的此项检查满足要求，否则不满足要求。

检查步骤

检查该邮件子系统服务器 Exchange Server 2003 是否能开启系统审计功能。如图 6.13 所示，“启用主题日志记录和显示”及“启用邮件跟踪”功能已经启用。

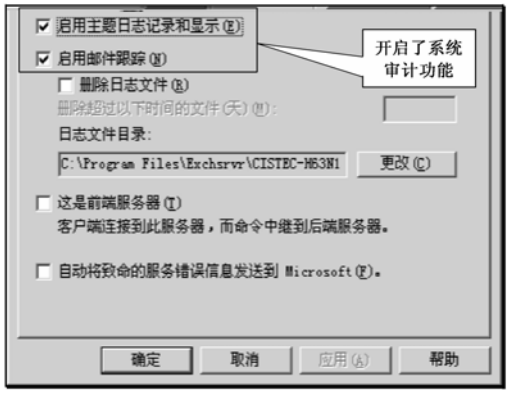


图 6.13　系统审计日志设置检查

检查结论：该邮件系统审计范围设置项符合检查要求。

（2）检查主要应用系统，查看其审计策略是否覆盖了系统内重要的安全相关事件，如用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为、系统资源的异常使用和重要系统命令的使用等。

检查目标：检查审计策略是否覆盖了系统内重要的安全相关事件。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

通过第（1）项的检查已经看到“天网”系统邮件服务器的安全审计日志已经启用。本项检查是进行该项功能的细化和核实的。为此，需要查看邮件服务器 Exchange Server 2003 中审计日志记录里可以包含的内容。本实验中选择的是常用的 POP3 通信协议。

检查步骤

进入“诊断日志记录”，检查该邮件子系统服务器 Exchange Server 2003 中日志记录所包含的内容，对 POP3 协议是否审计进行检查，如图 6.14 所示。

检查结论：该邮件系统审计策略事件覆盖设置项符合检查要求（事实上读者应当对其他的重要事件的安全审计日志逐一进行检查才可下结论）。

（3）检查主要应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）及事件的结果等内容。

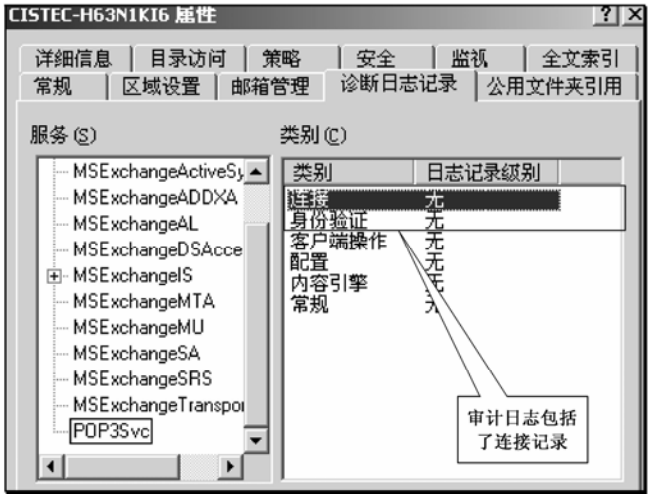


图 6.14　审计日志记录内容检查

检查目标：检查审计记录是否包括事件发生的日期与时间，触发事件的主体与客体等内容。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

通过在邮件服务器设置审计日志记录的保存位置，打开历史审计日志记录，先制造一个事件（如发送/接收一个邮件），然后查看日志是否包括了事件发生的主体与客体。如果包含，则邮件应用系统此项满足检查要求，否则不满足检查要求。

检查步骤

检查天网邮件子系统服务器 Exchange Server 2003 的历史日志记录事件，如图 6.15 所示，其中包含发送/接收邮件的 IP 地址（192.168.1.23/192.169.1.99）、邮件地址（qhxiang@tw.org）及发送时间（2008-3-23 7:47:9 GMT），等等。

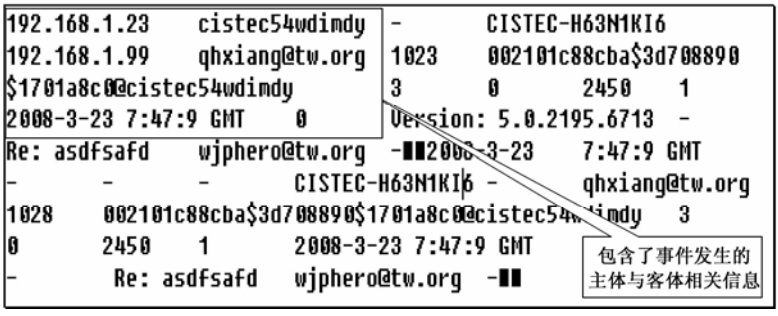


图 6.15　检查审计日志对事件发生全过程的记录

检查结论：该邮件系统审计记录中包含的内容项符合检查要求。

（4）检查主要应用系统，查看其是否为授权用户浏览和分析审计数据提供了专门的审计分析功能，并能根据需要生成审计报表。

检查目标：检查主要应用系统是否为授权用户浏览和分析审计数据提供了专门的审计分析功能。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

对于邮件应用系统而言，设计的实验是查看审计日志记录项，检查是否可以对已有的日志记录项进行重要性等级划分。如果可以划分则说明邮件应用系统此项满足检查要求，否则不满足检查要求。对于其他的应用系统，则应该检查是否可以进行审计查询、统计和分析等。

检查步骤

检查天网邮件子系统服务器 Exchange Server 2003 日志记录项是否可以划分重要性等级，进入该“诊断日志记录”卡后，可以看到对日志记录级别能进行“最高、中等、最低”等不同等级的划分设置，如图 6.16 所示。



图 6.16　审计分析功能检查

检查结论：该邮件系统审计记录重要性等级项功能设置符合检查要求，但默认设置是“无”。

（5）检查主要应用系统，查看其能否对特定事件指定实时报警方式（如声音、

E-mail 和短信等）。

检查目标：检查主要应用系统是否能对特定事件指定实时报警方式。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

对于邮件应用系统而言，特定事件包括对各种可疑邮件、垃圾邮件的报警，等等。设计的特定事件包括查看是否可以设置对邮箱存储或邮件传递的限制，以及当邮件存储达到限度时的报警功能。如果可以设置，则邮件应用系统此项满足检查要求，否则不满足检查要求。

检查步骤

检查天网邮件子系统服务器 Exchange Server 2003 是否可以设置对邮箱存储或邮件传递的限制，以及当邮件存储达到限度时的报警功能，如图 6.17 所示。为简单起见，在实验中设置邮箱的大小为 1KB，在实际工作中当然不会设置这样小的值。

检查结论：该邮件系统对重要安全事件报警项符合检查要求。

4．剩余信息保护现场检查

第 3 级安全测评要求对应用安全的剩余信息保护检查共有 2 项，且均为对现场文档检查。

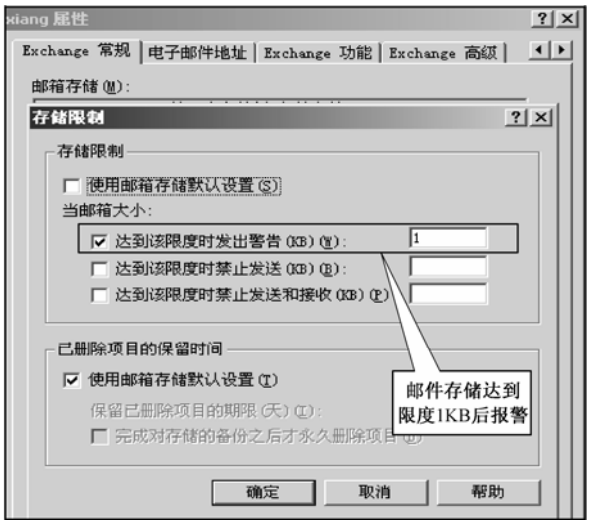


图 6.17　特定事件报警设置检查

（1）检查设计/验收文档，查看其是否有系统在释放或在分配鉴别信息所在存储空间给其他用户前如何将其进行清除（无论这些信息是存放在硬盘上还是在内存中）的描述。

（2）检查设计/验收文档，查看其是否有关于释放或重新分配系统内文件、目录和数据库记录等资源所在存储空间给其他用户前进行清除的描述。

5．通信完整性现场检查

第 3 级安全测评要求对应用安全的通信完整性检查只有 1 项，也属于文档检查。

检查设计/验收文档，查看其是否有通信完整性的说明，如果有，则查看其是否有根据校验码判断对方数据有效性的描述，以及用散列（Hash）密码计算报文验证码的描述。

第 3 级安全测评要求没有对应用安全通信的保密性等进行现场检查的要求。

6．软件容错现场检查

第 3 级安全测评要求对应用安全的软件容错检查只有 1 项。

检查主要应用系统，查看业务系统是否对通过人–机接口输入（如用户界面的数据输入）或通过通信接口输入的数据进行了有效性检验；是否在故障发生时能自动保护当前所有状态信息。

检查目标：检查主要应用系统，查看业务系统是否对通过人–机接口输入（如用户界面的数据输入）或通过通信接口输入的数据进行了有效性检验。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

为了对邮件应用系统进行软件容错检查，下面设计了两个实验：一是在邮件子系统客户端创建新的邮件账户，同时输入不合法的邮件地址，查看系统能否自动检测出不合法信息；二是通过写邮件过程中的强制关闭系统和重新启动系统，来检查系统是否能保护中断前的状态信息。如果能保护这些信息，则邮件应用系统此项满足要求，否则不满足要求。

检查步骤

① 检查该邮件子系统服务器客户端是否对不合法的邮件地址进行了检测。例如，发送的邮件地址中未带“@”（cistectw.org），如图 6.18 所示。

② 验证系统能否在故障发生时自动保护当前所有状态信息。使用 Outlook 邮件终端登录，编写一封电子邮件，然后非法关闭机器。再重新开机后登录到电子邮件系统，发现刚撰写的电子邮件丢失了，如图 6.19 所示。

检查结论：该邮件系统通过人–机接口输入数据的有效性检验项符合检查要求；但系统不能在故障发生时自动保护当前所有状态信息，不满足检查要求。

7．资源控制现场检查

第 3 级安全测评要求对应用安全的资源控制检查共有 3 项。

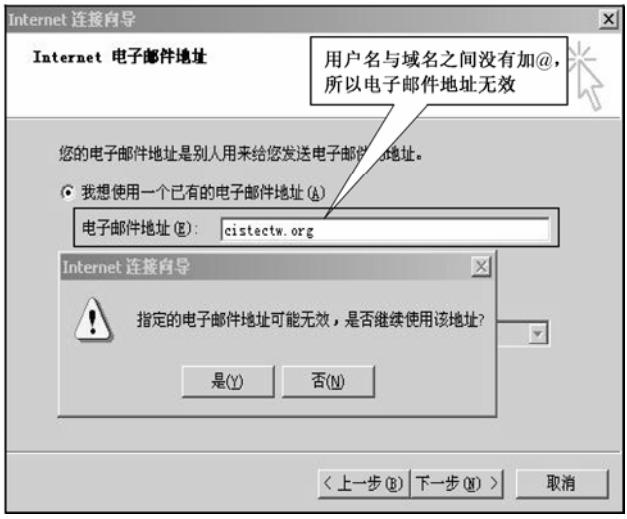


图 6.18　邮件地址合法性检查

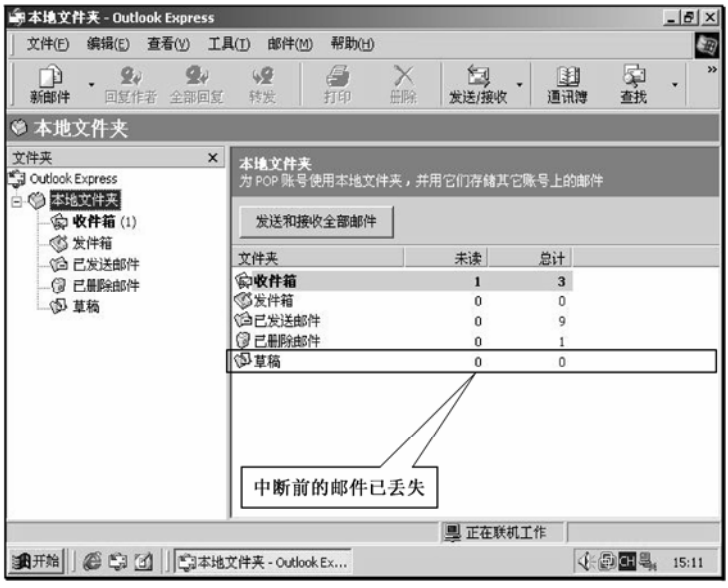


图 6.19　系统意外中断时自动保护状态检查

（1）检查主要应用系统，查看是否限制了单个账户的多重并发会话功能；系统是否有最大并发会话连接数的限制，是否对一个时间段内可能的并发会话连接数进行了限制；是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源。

检查目标：检查系统是否有最大并发会话连接数的限制，是否对一个时间段内可能的并发会话连接数进行了限制。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

查看是否可以设置在同一时间内并发接连到邮件服务器 Exchange Server 2003 的用户数量，如果可以设置，则邮件应用系统此项满足要求，否则不满足要求。顺便指出，该项检查也可以对邮件服务器是否能抵御常见的 DDOS 攻击进行验证。

检查步骤

检查天网邮件子系统服务器 Exchange Server 2003，是否设置了在同一时间内同时连接到邮件服务器的客户端数量。如图 6.20 所示，可以看到，在“限制连接数不超过”和“连接超时（分钟）”功能模块上分别设置了“20 个”连接和“10 分钟”超时限制。

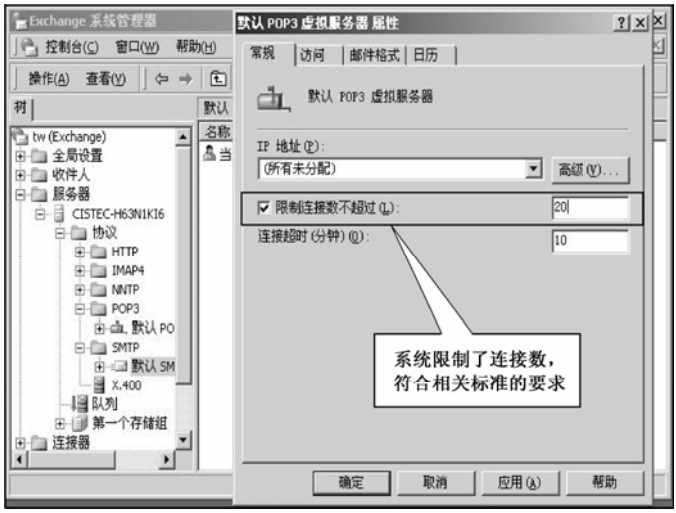


图 6.20　邮件用户连接数及连接超时设置检查

检查结论：该邮件系统最大并发会话连接数的限制项符合检查要求。

（2）检查主要应用系统，查看是否对一个访问账户或一个请求进程占用的资源分配了最大限额和最小限额。

检查目标：检查主要应用系统，查看是否对一个访问账户或一个请求进程占用的资源分配了最大限额和最小限额。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

查看是否可以设置用户邮箱存储、发送和接收邮件的大小，同时是否可以对每封邮件发送人数进行设置，如果可以设置，则邮件应用系统此项满足要求，否则不满足要求。

检查步骤

检查天网邮件子系统服务器 Exchange Server 2003，是否可以设置用户邮箱存储、发送和接收邮件的大小，同时是否可以对每封邮件发送人数进行设置。如图 6.21 所示，发现该邮件服务器对“限制邮件大小”、“限制会话大小”、“限制每个连接的邮件数”和“限制每封邮件的收件人数”等均进行了设置。

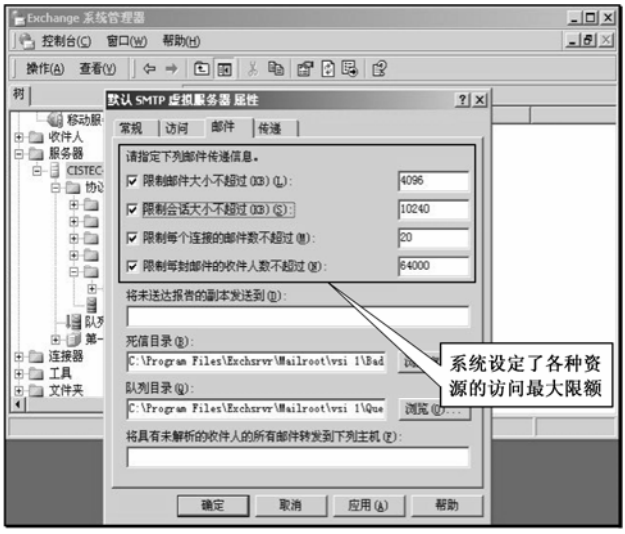


图 6.21　邮件使用限制的配置检查

检查结论：该邮件系统的一个访问账户或一个请求进程占用的资源分配最大限额和最小限额项符合应用检查要求。

（3）检查主要应用系统，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警。

检查目标：检查是否有服务水平最小值的设定。

检查对象：“天网”系统中心机房。

检查环境：Exchange Server 2003。

检查方案：

技术路线

查看是否可以设置用户邮箱存储、发送和接收邮件的大小，是否可以对超过上限值的情况进行报警的设置，如果可以设置，则邮件应用系统此项满足要求，否则不满足要求。

检查步骤

检查天网邮件子系统服务器 Exchange Server 2003，是否可以设置用户邮箱存储、发送和接收邮件的大小，是否对超过上限值的情况进行了报警。如图 6.22 所示，发现实际对“达到该限度时发出警告”和“达到该限度时禁止发送”两个功能均进行了设置。

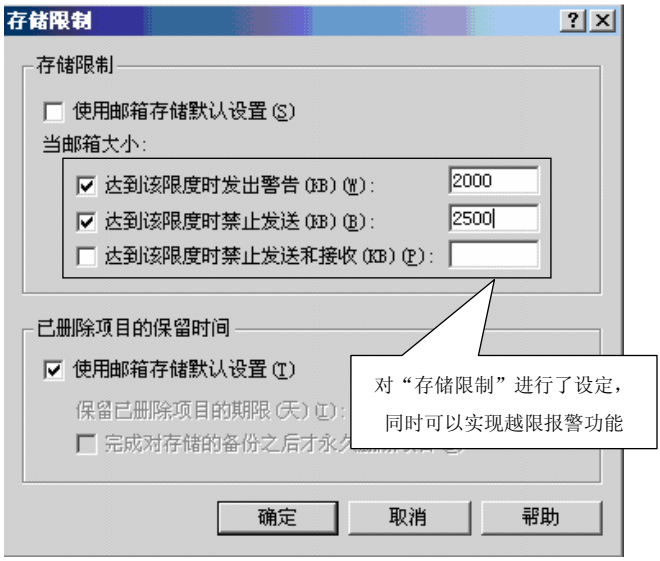


图 6.22　邮件存储服务水平及报警设置检查

检查结论：该邮件系统服务最低水平值项符合应用安全测评资源控制检查要求。

请读者注意，国家第 3 级安全标准中没有对“通信保密性”和“抗抵赖”的检查要求。

至此，我们以邮件应用系统为例，按标准完成了应用安全现场检查的所有任务。下面进入应用安全的测试阶段。依然以邮件服务器为例来进行这项“自由动作”的比赛。

6.2.3　应用安全测试

1．身份鉴别测试

第 3 级安全测评要求对应用安全的身份鉴别测试共有 2 项。

（1）测试主要应用系统，可通过以某注册用户身份登录系统，查看登录是否成功，验证其身份标识和鉴别功能是否有效。

测试目标：测试身份标识和鉴别功能是否有效。

测试对象：“天网”邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

安装 Exchange Server 2003，按要求配置好 DNS 和 Exchange Server 2003。设计的方案是常规性的实验，即在邮件子系统客户端安装 Outlook，并在服务器上创建一个新的邮件用户，然后在客户端通过创建的用户名和密码登录，如果登录成功，说明邮件应用系统此项符合测评要求；否则不符合测评要求。读者也可以通过非常规的方法来测试，

如授权用户以错误口令登录，或者使用像前几章介绍过的绕过认证方法等方式。

测试步骤

① 创建一个 xiang 用户，如图 6.23 所示。



图 6.23　创建新用户

② 对该用户分配用户口令，如图 6.24 所示。

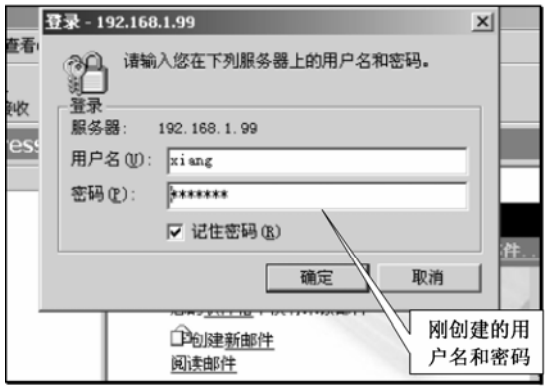


图 6.24　创建用户名和密码

③ 使用该用户名和口令登录，如图 6.25 所示。

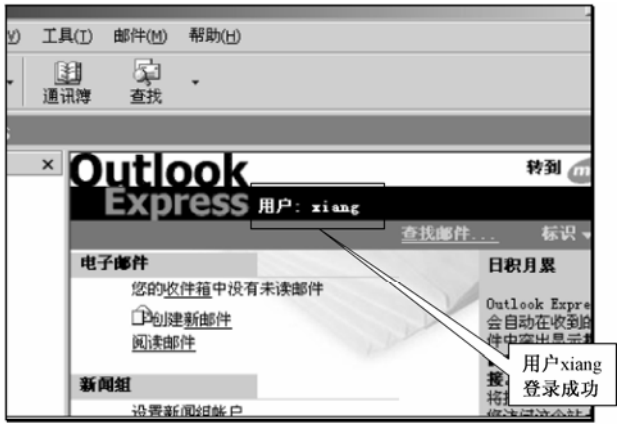


图 6.25　验证用户名及密码

测试结论：该邮件系统身份标识和鉴别功能项符合测试要求。

（2）测试主要应用系统，验证其登录失败处理功能是否有效。

测试目标：验证登录失败处理功能是否有效。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

初看起来这是一个非常简单的测试，如可以反复用错误口令或用户名登录邮件系统来测试其处理登录失败的功能。但为了细化测试粒度，新设计的方案是：在邮件子系统客户端安装 Outlook，并在服务器上设置限制某一用户登录的时间（见现场检查环节“身份鉴别”（5）的实验），然后通过客户端在此时段内登录邮件服务器，如果登录不成功则说明邮件应用系统此项符合测评要求，否则不符合测评要求。

测试步骤

根据服务器上设置的一个限制登录时间（不允许登录的时间段），通过客户端在此时段内登录服务器，然后查看是否成功。如图 6.26 所示，Outlook 提示了登录邮件服务器时出错的详细信息。要注意错误信息虽然是“密码不对”，但实际上是由于事先设置了限制登录的时间而引起的。

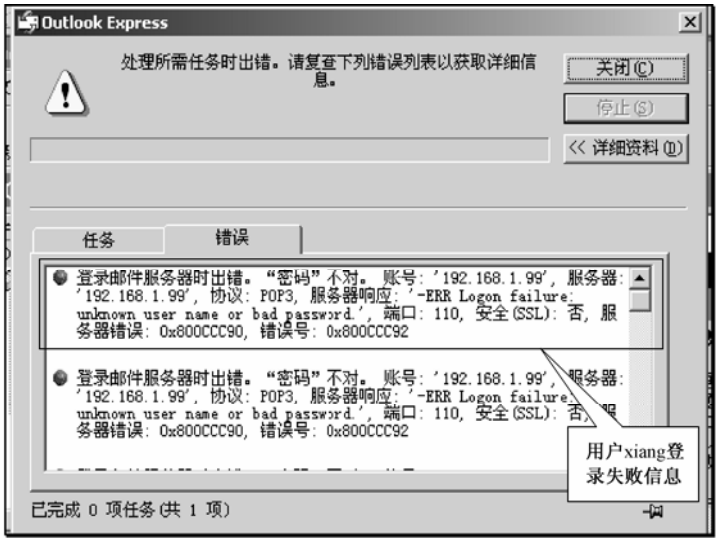


图 6.26　登录失败处理功能测试

测试结论：该邮件系统登录失败处理功能项符合测试要求。

2．访问控制测试

第 3 级安全测评要求对应用安全的访问控制测试共有 4 项。

（1）测试主要应用系统，通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效。

测试目标：测试用户权限是否受到应用系统的限制。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

可以继续使用应用安全测试中身份鉴别测试实验的设计思路，即在邮件子系统客户端安装 Outlook，在服务器上设置禁止某一用户登录的时间，然后通过客户端在此时段登录邮件服务器，检查登录结果，如果登录不成功则说明邮件应用系统此项符合测评要求，否则为不符合测评要求。

测试步骤

在客户端找服务器上设置的一个禁止登录时间段登录服务器，然后查看普通用户“xiang”是否能够登录成功，如图 6.27 所示。

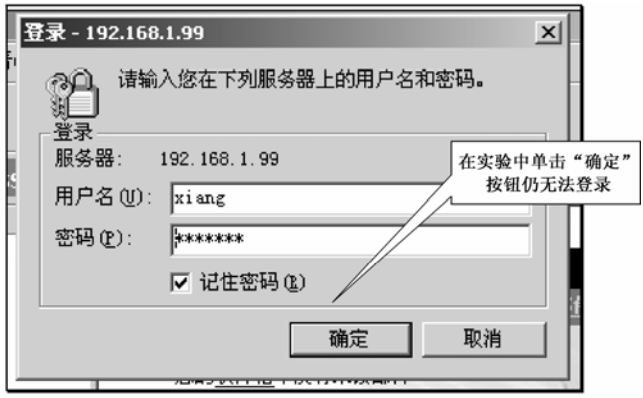


图 6.27　普通用户访问权限测试

测试结论：该邮件应用系统限制用户权限项符合测试要求。

（2）测试主要应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效。

测试目标：测试用户对系统功能进行操作和数据访问的权限是否有效。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

在邮件子系统客户端安装 Outlook，设定一个用户发送邮件的大小上限为 1KB，在客户端上以此用户名义向另一个用户发送大小超过 1KB 的邮件，查看接收邮件方能否

收到此邮件，如果能收到，则说明邮件应用系统此项不符合测评要求，否则为符合测评要求。

测试步骤

① 设置用户 li 发送邮件大小的最大值为 1KB，如图 6.28 所示。



图 6.28　用户使用权限设置

② 通过 li@cistec.org 用户向 keke@cistec.org 用户发送大小超过 1KB 的邮件，如图 6.29 所示。



图 6.29　用户使用权限设置测试（1）

③ 查看 keke@cistec.org 能否收到邮件。如图 6.30 所示，Outlook 提示收件方“keke”没有未读邮件，由此说明这个限制措施是有效的。

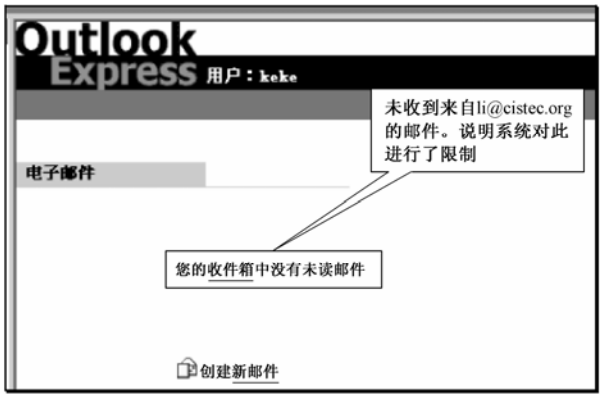


图 6.30　用户使用权限设置测试（2）

测试结论：该邮件应用系统用户对系统功能进行操作和数据访问的权限有效，此项符合测评要求。

（3）测试主要应用系统，验证系统对默认用户访问权限的限制是否有效。

测试目标：测试是否可以通过默认用户进行操作。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

通过默认用户（默认密码）登录，并让该用户进行操作（包括合法和非法的操作）。为此，在客户端上设定一个用户为默认登录用户，然后再以此用户名义登录，如果登录成功并能进行各种操作，则说明邮件应用系统此项不符合测评要求，否则说明符合测评要求。

测试步骤

设置 xiang@cistec.org 默认用户，通过该默认用户登录后，可以进行各项操作，如图 6.31 所示。

测试结论：该邮件系统默认用户的操作超出限制，不符合应用安全测评访问控制测试的要求。

（4）渗透测试主要应用系统，测试自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体以及它们之间的操作（如试图绕过系统访问控制机制等操作）。

测试目标：测试自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体以及它们之间的操作。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

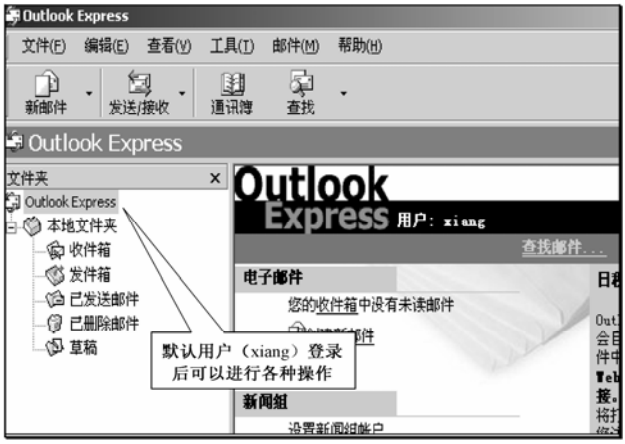


图 6.31　默认用户访问权限测试

测试方案：

技术路线

为了进行该项测试，需先设置邮件系统的访问控制机制，具体方案如下：在邮件系统中设置一个用户不能接收另一个用户邮件的传递限制功能，然后在邮件子系统客户端安装 Outlook，用后者用户向前者用户发送一封邮件，查看前者用户能否收到此邮件，如果能收到，则说明邮件应用系统此项不符合测评要求，否则符合测评要求。

测试步骤

① 设定用户 xiang@tw.org 不能接收从用户 xqh@tw.org 发送的邮件（在“邮件限制”模块中选择“来自任何人，除 xqh”单选项），如图 6.32 所示。



图 6.32　用户操作限制设置

② 由用户 xqh 向 xiang 发送一封邮件，如图 6.33 所示。

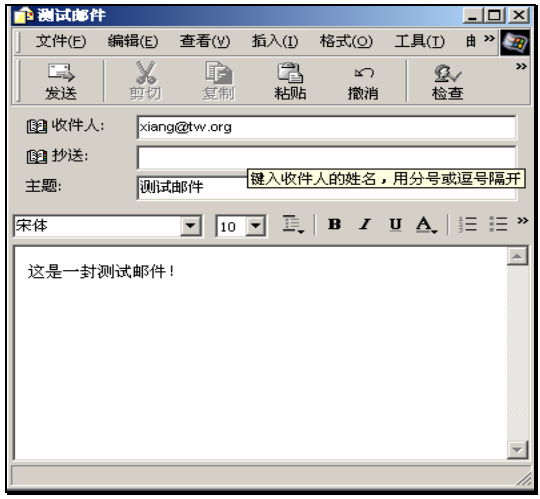


图 6.33　用户操作限制测试（1）

③ 查看用户 xiang 的邮箱，即 xiang@tw.org 邮箱，如图 6.34 所示，未见收到来自 xqh@tw.org 的邮件，说明操作无法绕过访问控制机制。

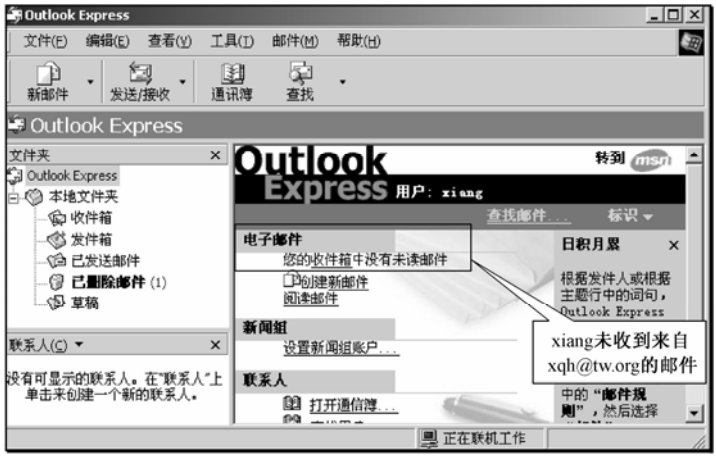


图 6.34　用户操作限制测试（2）

测试结论：该邮件系统自主访问控制的覆盖范围项符合应用安全测评访问控制测试要求。

3．安全审计测试

第 3 级安全测评要求对应用安全的安全审计测试共有 3 项。

（1）测试主要应用系统，验证审计进程是否受到保护。

测试目标：验证审计进程是否受到保护。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

为了测试审计进行是否受到保护，可以通过非法终止审计功能或修改其配置，来测试是否能将日志记录关闭。我们的方案是将“启用主题日志记录和显示”、“启用邮件跟踪”两个模块均设置成“不启用”（在多选框中不钩选），如果能操作成功，则说明日志进程未受到保护，邮件应用系统的安全实际功能不符合测评要求。

测试步骤

修改日志记录配置，停用日志记录，如图 6.35 所示。

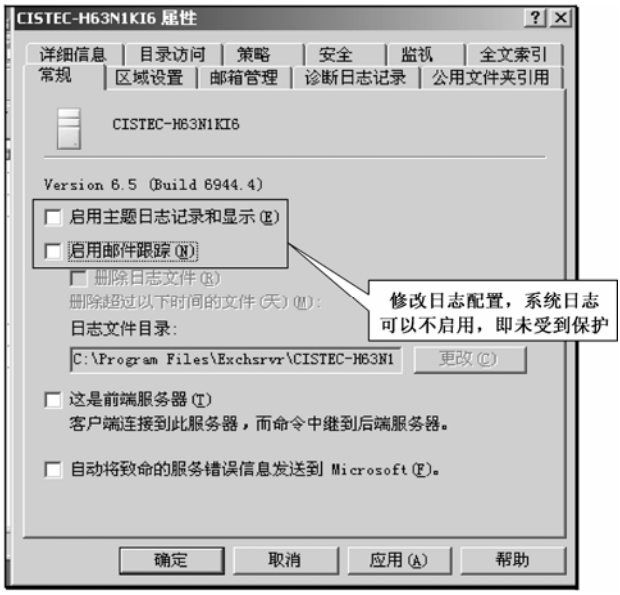


图 6.35　审计功能设置测试

测试结论：该邮件系统审计进程不符合应用安全测评安全审计测试要求。（事实上，为了进一步验证是否真的停用了日志审计功能，读者还应当进行另外一些操作，如发送邮件等，然后检查日志记录，由于这是一个常规性的操作，我们将其留给读者自行练习。）

（2）测试主要应用系统，在系统上以某个用户名义进行操作，并试图产生一些重要的安全相关事件（如鉴别失败等），以此测试安全审计的覆盖情况和记录情况与安全测评要求是否一致。

测试目标：测试安全审计的覆盖情况和记录情况与安全测评要求是否一致。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

在系统上，通过某一用户向另一个用户发送一封邮件，查看日志记录是否包括了时间、客户端地址、客户端主机名、服务器地址、接收地址和事件 ID 等。如果此记录和刚发送邮件事件一致，则符合邮件应用系统对此项的安全测评要求，否则不符合安全测评要求。

测试步骤

① 用户从邮箱 xqh@tw.org 向邮箱 xiang@tw.org 发送一封邮件：“这是一封测试邮件”，如图 6.36 所示。



图 6.36　产生一个邮件发送事件

② 立即查看发送邮件系统中的日志文件。从日志中可以看到上面记载了刚刚完成操作的全部记录，如邮件的发送/接收方地址和时间等，如图 6.37 所示。



图 6.37　事件全过程记录测试

测试结论：该邮件系统安全审计的覆盖情况和记录情况与要求一致，符合应用安全

测评要求。

（3）测试主要应用系统，验证安全审计的保护情况与安全测评要求是否一致。

测试目标：验证安全审计的保护情况与安全测评要求是否一致。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

通过在系统上以某个系统用户的名义进行删除、修改并覆盖原审计记录的操作，如果能成功覆盖，则邮件应用系统此项不符合安全测评要求，否则满足安全测评要求。

测试步骤

① 首先调出一个日志文件，修改已有日志记录，并以同样的文件名（20080323）保存，覆盖原有记录，如图 6.38 所示。

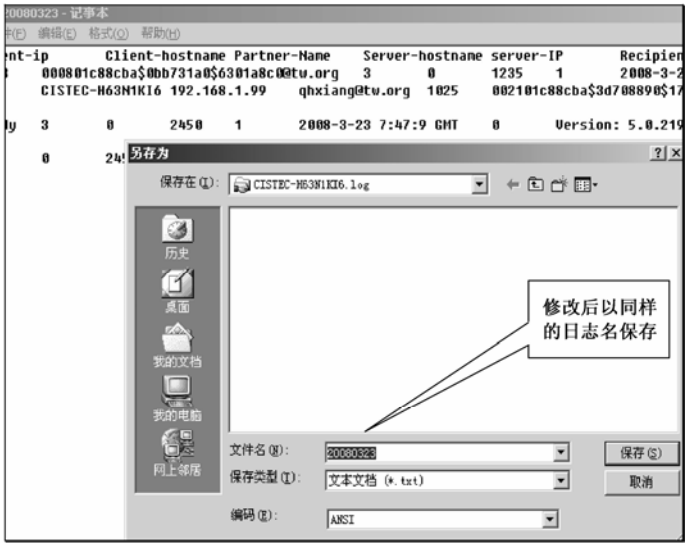


图 6.38　审计日志防篡改测试（1）

② 立即发现不能保存该文件，如图 6.39 所示。



图 6.39　审计日志防篡改测试（2）

测试结论：该邮件系统安全审计的保护情况与安全测评要求一致，符合应用安全测

评安全审计的测试要求。

4．剩余信息保护测试

第 3 级安全测评要求对应用安全的剩余信息保护测试只有 1 项。

测试主要应用系统，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，在被释放或重新分配给其他用户前得到完全清除）。

测试目标：验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，在被释放或重新分配给其他用户前得到完全清除）。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

该测试的基本思想是以某用户名义登录系统并进行操作，在该用户退出系统后再用另一用户名登录，然后读取、修改或删除前一用户产生的文件、目录和数据库记录等资源，再查看操作是否成功。为此，可以通过 OWA（Outlook Web Access）邮箱，退出后再次登录，如果上一次登录信息以及使用信息不存在，则说明邮件应用系统此项符合安全测评要求，否则不符合安全测评要求。

测试步骤

使用“keke”用户登录，退出后，重新登录，查看残余信息是否存在。从图 6.40 可以看到，在目录树中有关“keke”的信息均未出现。

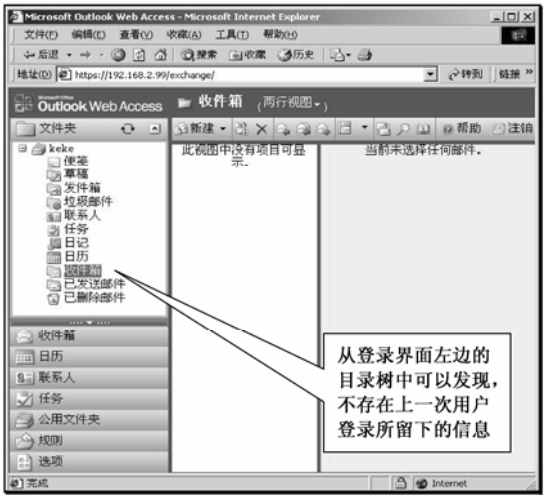


图 6.40　剩余信息保护测试

测试结论：该邮件系统剩余信息保护功能项符合应用安全测评剩余信息保护测试的要求。

5．通信完整性测试

第 3 级安全测评要求对应用安全的通信完整性测试只有 1 项。

测试主要应用系统，通过获取通信双方的数据包，查看通信报文是否含有加密的验证码。

测试目标：测试主要应用系统，通过获取通信双方的数据包，查看通信报文是否有验证码。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

先安装网络协议分析软件 Ethereal，然后在邮件系统客户端安装 Outlook，并在两个客户端发送和接收邮件，同时启用 Ethereal 进行监听和抓包操作，以此查看发送邮件的过程是否包括在发送邮件之前申请建立连接的整个过程中，是否含有加密的验证码。

测试步骤

① 打开 Ethereal 软件的操作界面，对其网卡进行设置，由于本实验是在虚拟机上实现的，所以选择虚拟机网卡接口，如图 6.41 所示。

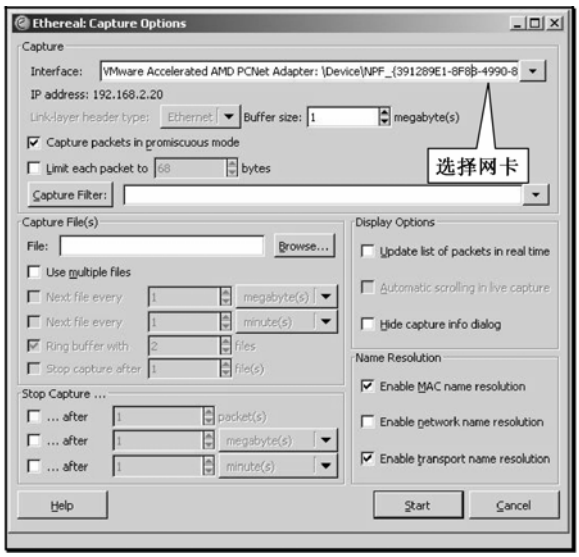


图 6.41　Ethereal 配置

② 使用 Ethereal 捕获通信数据包，单击“start”按钮，开始对应用系统进行数据捕获。由于在此之前应用系统没有与其他主机进行通信，因此从 Ethereal 软件界面中无法

看到任何有关于数据包的信息。然后，我们通过访问应用系统，与应用系统进行数据通信，再查看捕获的数据包信息，如图 6.42 所示。

③ 查看通信数据包，查找验证码，通过 filter 选择与应用系统相关的通信协议查看其报文是否有加密验证码，从图 6.43 可以看到，在整个申请连接的过程中，用户名（USER keke）、应答（Response OK）、用户口令（PASS 654321）、应答成功（User successfully logged on）等一系列操作全是明文显示（明文验证码）。

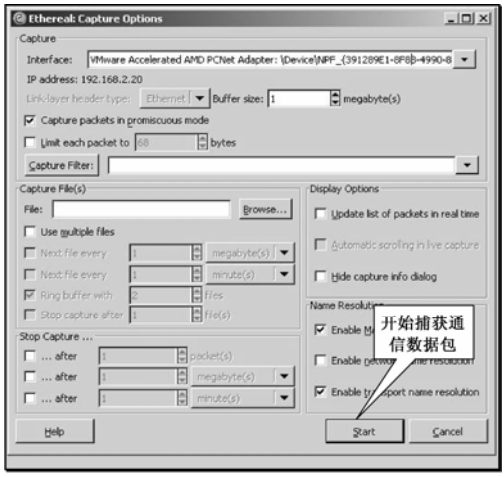


图 6.42　启动 Ethereal 捕获数据包

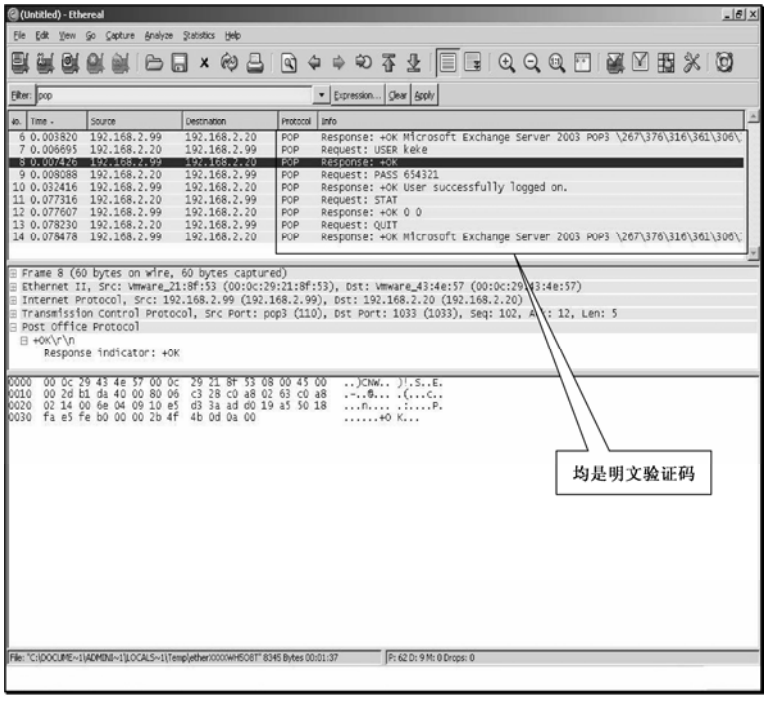


图 6.43　通信保密性测试（1）

测试结论：该邮件应用系统通信报文没有对验证码进行加密处理，不符合应用安全测评通信完整性测试的要求。

6．通信保密性测试

第 3 级安全测评要求对应用安全的通信保密性测试只有 1 项。

测试主要应用系统，通过通信双方数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行了会话初始化的验证（如 SSL 建立加密通道前是否利用密码技术进行了会话初始的验证）；查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。

测试目标：测试主要应用系统，通过通信双方数据包的内容，查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

安装网络协议分析软件 ethereal。在邮件系统客户端安装 Outlook，并使邮件客户端在发送邮件之前先建立连接，同时操作服务器启用协议分析进行监听，查看建立连接和报文的密码是否进行了加密处理。如果通过协议分析软件能看到未经加密的登录口令，则邮件应用系统此项不符合安全测评要求，否则满足安全测评要求。

测试步骤

① 打开 Ethereal 软件的操作界面，对其网卡进行设置。由于本实验是在虚拟机上实现的，所以，选择虚拟机网卡接口（见图 6.41）。

② 捕获通信数据包，单击“start”按钮，开始对应用系统进行数据捕获。由于此时应用系统没有与其他主机进行通信，从 Ethereal 软件界面中无法看到任何有关数据包的信息。因此，再通过用户名为 keke、密码为 654321，登录访问应用系统，与应用系统进行数据通信，查看捕获的数据包信息，如图 6.42 所示。

③ 通过通信数据包，查看对用户密码有无加密设置。从图 6.44 中可以看出，通信报文中的用户口令仍然清晰可辨（明文显示）。

测试结论：在该邮件系统通信过程中，整个报文或会话过程未采用加密功能，不符合安全测试要求。

7．抗抵赖测试

第 3 级安全测评要求对应用安全的抗抵赖测试只有 1 项。

测试主要应用系统，通过双方进行通信，查看系统是否在请求的情况下为数据原发者或接收者提供了数据原发证据的功能；是否在请求的情况下为数据原发者或接收者提供了数据接收证据的功能。

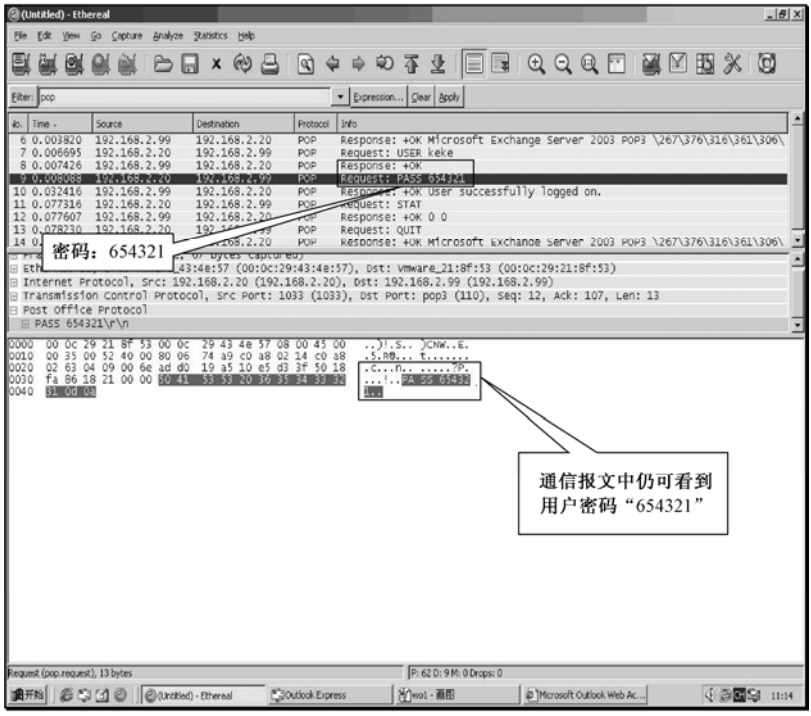


图 6.44　通信保密性测试（2）

测试目标：验证主要应用系统能否在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

在客户端之间对用户发送一封邮件，查看日志记录里是否存在发送邮件的详细信息，如日期、原发者和接收者，如果存在，则说明邮件应用系统此项符合安全测评要求，否则不满足安全测评要求。

测试步骤

操作 wjphero@tw.org 向 qhxiang@tw.org 发送邮件后，通过查看系统日志来验证是否存在该行为的详细信息，如图 6.45 所示。

测试结论：该邮件系统能为数据原发者或接收者提供数据接收证据的功能，符合应用安全测评抗抵赖测试要求。

这里要提醒读者注意的是，这种测试严格地讲应该通过“无法销毁”的测试来验证其“抗抵赖”功能。上述实验中仅仅说明日志中有相关的操作记录。但是正如在前面的实验中已经看到的，日志本身的保护非常重要，如果事先没有启动日志审计或对日志进

行篡改操作，则无法验证其“抗抵赖”的功能。比较好的测试方法是在应用软件上使用数字证书等工具。

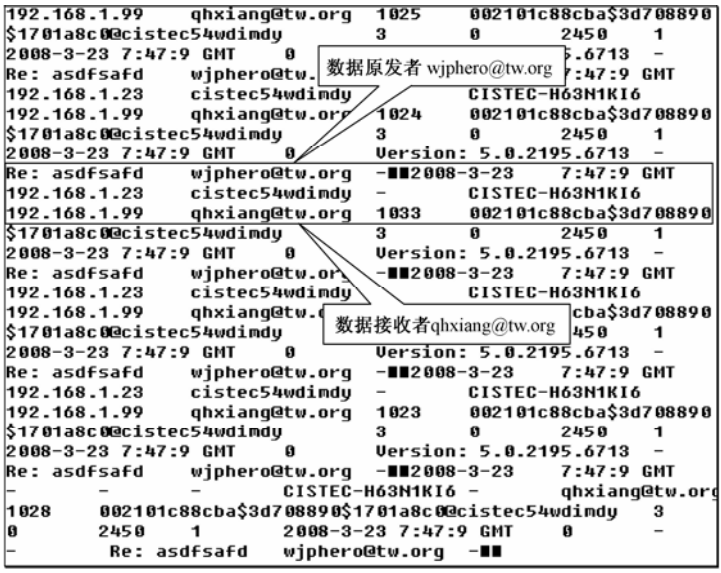


图 6.45　抗抵赖性测试

8．软件容错性测试

第 3 级安全测评要求对应用安全的软件容错测试只有 1 项。

测试主要应用系统，验证系统人–机接口有效性检验功能是否正确。

测试目标：验证主要应用系统人–机接口有效性检验功能是否正确。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

在客户端新建一个用户，输入不合法的邮件地址，以此验证系统能否检测出不合法信息，同时查看系统在新建用户时能否进行回置操作。

测试步骤

① 新建邮件用户，输入非法邮件地址“cistectw.org”，如图 6.46 所示。

② 验证系统能否按照操作序列进行正确的回退。通过多步的操作，记录下每一步的操作，然后进行回退，如图 6.47 所示。

测试结论：该邮件系统人–机接口有效性检验功能符合应用安全测评软件容错测试的要求。

9．资源控制测试

第 3 级安全测评要求对应用安全的剩余信息保护测试共有 2 项。

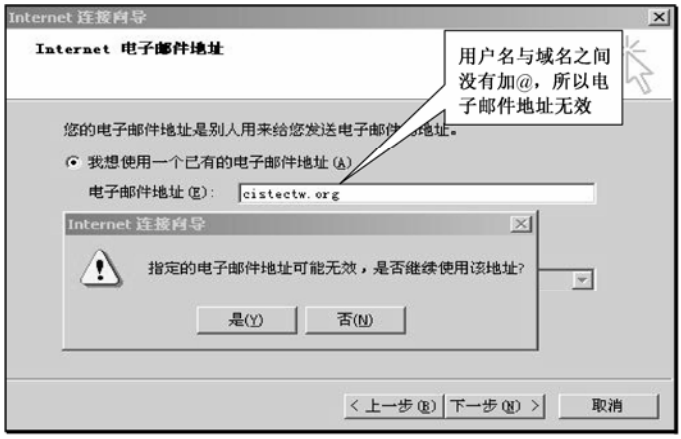


图 6.46　创建不合法邮件地址测试

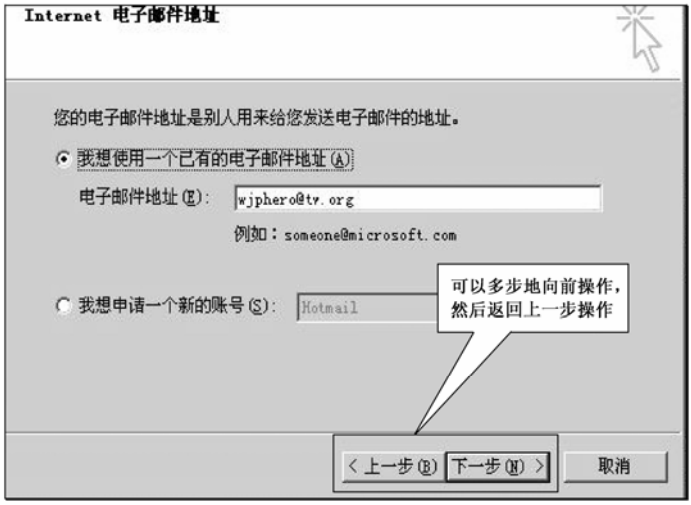


图 6.47　回退操作测试

（1）测试主要应用系统，验证系统能否正确地限制单个账户的多重并发会话数。

测试目标：主要应用系统能否正确地限制单个账户的多重并发会话数。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

以同一个账户同时在多个客户端登录，查看是否能登录成功。如果成功登录则说明邮件应用系统此项不符合安全测评的要求，否则符合安全测评的要求。

测试步骤

在两台不同地址客户端以同一个邮件用户身份登录，查看是否能成功登录，并进行各种操作，如图 6.48 和图 6.49 所示。

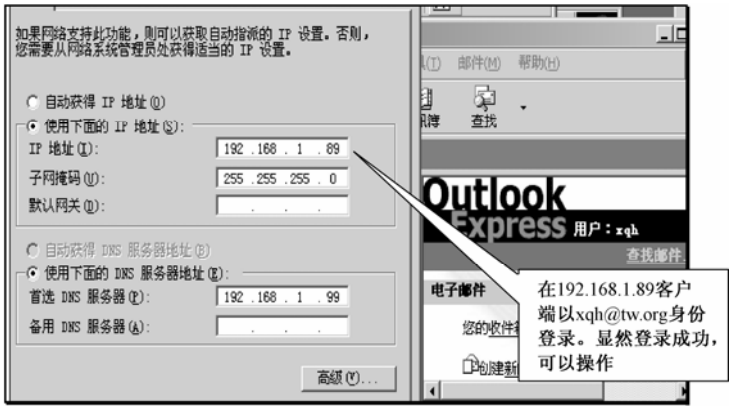


图 6.48　资源控制测试（1）

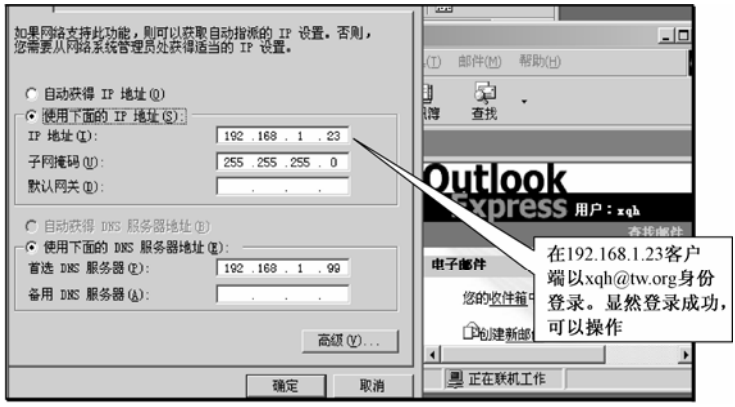


图 6.49　资源控制测试（2）

测试结论：该邮件系统不能正确地限制单个账户的多重并发会话数，不符合应用安全测评资源控制测试的要求。

（2）测试主要应用系统，使服务水平降低到预先规定的最小值，以验证系统能否正确检测并报警。

测试目标：测试主要应用系统，使服务水平降低到预先规定的限制值，以验证系统能否正确检测并报警。

测试对象：“天网”系统邮件服务器。

测试环境：“天网”系统中心机房。

测试方案：

技术路线

在客户端设置一用户邮箱的存储限制值，然后用另一用户身份向此用户发送大小超过该限制值的邮件，并在服务器上设置警告发出的时间间隔为 15 分钟，查看发送方是否能收到警告邮件。

测试步骤

① 设置用户 xiang@tw.org 的邮箱存储限制值为 10KB，如图 6.50 所示。

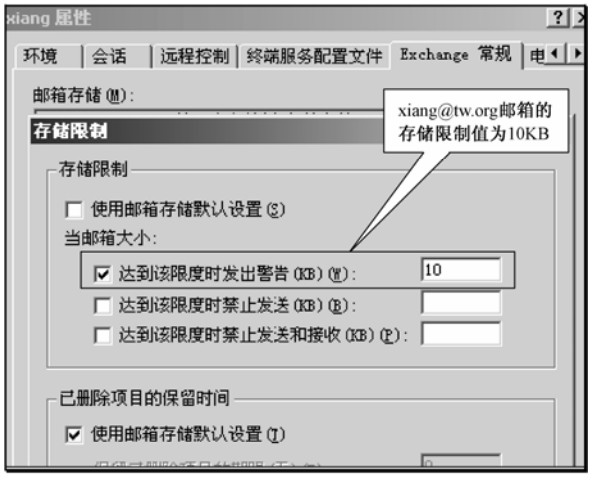


图 6.50　资源存储限制值设置

② 设置警告时间，如图 6.51 所示。

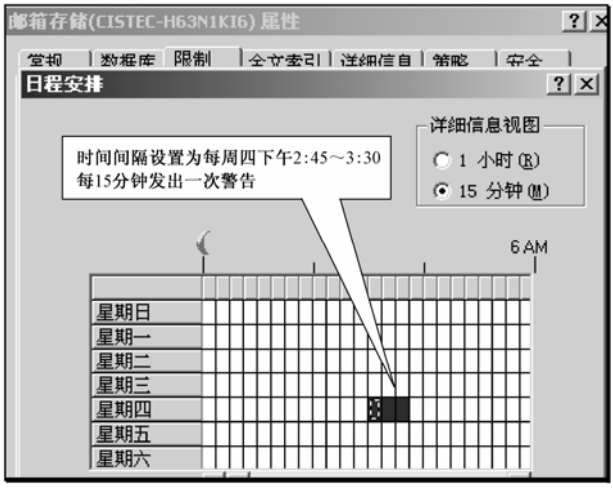


图 6.51　资源存储控制的报警设置

③ 由 xqh@tw.org 向 xiang@tw.org 发送一封大小超过 10KB 的邮件，等待 15 分钟后，收到如图 6.52 所示的警告邮件。

测试结论：该邮件系统能对服务水平降低到限制值时发出警告，符合应用安全测评资源控制测试的要求。

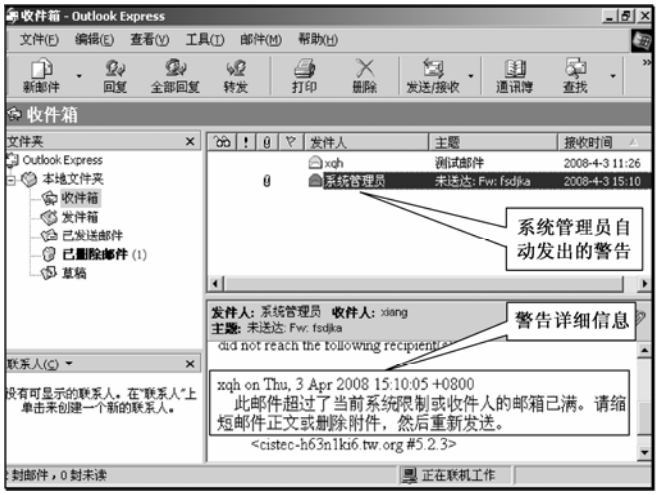


图 6.52　报警设置测试

至此我们全部完成了对应用安全的测试工作。读者应当在这部分工作结束后，将其测试记录整理成“天网应用系统安全测试记录”，并与“问卷调查”和“现场检查”的技术报告合并在一起，形成“天网应用系统安全测评技术报告”。

6.3　本章小结

- 应用安全测评的三种方法
- 身份鉴别测评
- 访问控制测评
- 安全审计测评
- 剩余信息保护测评
- 通信完整性测评
- 通信保密性测评
- 抗抵赖测评
- 软件容错测评
- 资源控制测评

尾声：史上最“万能”的机器

恐龙称霸地球 15000 万年，人类登台迄今才 300 万年，有文字的人类文明史更只有区区 6000 年。

但人类却在其成为万物之灵的瞬间里，做了无数奇异的梦:

千里眼，顺风耳;

像鸟一样在天上自由飞翔;

奔向迷人的月宫;

天上一日，人间千年（时光隧道）;

永动机;

……

在今天看来，人类的梦想有几种:

已经实现了的，如“千里眼、顺风耳”、“在天上飞”、“奔月”，等等，这种情况很多。

迄今还没有实现的，如到未来的时光隧道；被科学证明不可能实现的，如“永动机”。

当然，还有一种情况，就是人类可能做梦也没有想到过，却已经变成现实了的，如核弹、Internet 等。

人类也许没有像幻想“永动机”那样去设想一种“万能机”。如果问史上最“万能”的机器是什么，现在的回答只能是“计算机”了。

与迄今人类发明的其他伟大机器相比，计算机是最“万能”的。它为什么万能？因为它有了“灵魂”，使得它才如此灵活多变和多才多艺。它的“灵魂”源自什么？软件。灵魂附于躯体，软件附于硬件。

当我们谈“应用”（applications）时，一般就是谈软件。“应用”这个词最初是相对于“系统”（system）而言的，因此我们才说应用软件（简称“应用”）。撇开名称的来历不说，“应用”这个词实在是难以准确表述它的重要特征——让计算机“72 变”的关键所在。不知是否是微软意识到了这点，在它的.NET 推出的时候，其开发环境就不仅仅有过去对应于“应用”的“项目（project）”，更有了“解决方案（solution）”。

似乎还不够。有没有反映“万能”机器“万变”软件的一个更贴切的新名称？对象（objects）？构件（components）？不合适，服务（services）？仍不合适……

观感

（1）应用安全测评与“数据安全”、“主机安全”和“网络安全”等测评有什么相同和不同之处？

（2）操作系统的安全测评属于应用安全测评的范围吗？

（3）您认为一个应用软件在开发过程中要注意哪些环节才能够达到国家有关应用安全三级标准的要求？

（4）为什么应用安全的问题如此纷繁？

（5）请按照您的理解，设计并完成“访问控制”现场检查的第二项内容。

（6）如果您在使用 QQ、MSN 等及时通信系统，并且属于一个第 3 级的信息系统，请您给出它的安全测评要求。

（7）请将本章现场“动手检查”的部分整理成一个对 Exchange Server 2003 应用软件安全检查的报告。

（8）请将本章测试工作的记录进行归类整理，并与前面所形成的检查报告合并在一起，形成对 Exchange Server 2003 应用软件的安全测评报告。

第7章
资产识别





1666 年伦敦大火

阶级社会的驱动力可以用一句话来概括：我饿！风险社会的驱动力则可以用另一句话来概括：我怕！

——Ulrich Beck《风险社会》

序幕：伦敦大火启示录

1666 年 9 月 2 日凌晨，Thomas Bludworth 爵士被人从美梦中叫醒。仆人告诉这位睡眼惺忪的市长大人，国王查理二世位于伦敦大桥旁 Pudding 巷的御用面包坊起火了，让他尽快去查看一下。Thomas 市长心不甘情不愿地来到火灾现场，满不在乎地讲了一句粗俗的“名言”：“撒泡尿也可以把它扑灭”，然后就回到家中倒头呼呼大睡起来，他也许没有注意到窗外开始起风了……

接下来的几天，这座欧洲大陆最繁华的城市之一变成了人间炼狱：浓烟烈火、人喊马嘶，再加上隆隆的爆炸声。因为焦头烂额的查理二世不得不下令用爆破灭火方式开辟隔离带的方式来挽救剩下的房屋……当最后一缕火焰被扑灭之后，整个伦敦城仅有 1/5 的建筑得以幸存。

伦敦大火（The Great Fire of London）因人为疏忽而起，火借风势，蔓延全城，最后带来极为惨重的损失，这大概是“风险”一词最恰当的诠释了。从本章开始，将涉猎信息系统风险评估的各个环节。使得读者能够把自己的信息系统出现“火灾”的苗头消灭在萌芽之中，从而保证信息系统的长治久安。

要点：本章结束之后，读者应当了解和掌握

- 什么是风险？
- 风险评估有哪些环节？
- 什么是资产和资产识别？
- 资产识别有哪些环节？
- 资产识别最后要达到的效果是什么？

7.1 风险概述

20 世纪 80 年代，中国正准备进入工业化时代，西方发达国家则正准备从工业化向

信息化转型。但无论是工业化还是信息化，从社会学的角度来看都属于科技领域的名词。德国社会学家 U.Beck 在 1986 年出版了一本专著《风险社会》，提出了人类文明正在从“工业社会”向“风险社会”转变的理论。他的这一观点正得到越来越多的关注。当今世界上许许多多国家开始高度重视各个领域的“风险”，例如，新闻报道中常提及的自然灾害风险（如全球变暖的风险）、战争风险、金融风险等。



在中国的民间传说中，“风险”一词是古代渔民和海员最先使用的。由于在茫茫大海上航行的时候最忌讳的就是狂风大作，有风就有险，所以产生了这个术语。在西方，根据目前可以考证的资料来看，风险（risk）这个概念是由现代会计学之父、意大利数学家 Luca Pacioli 在 1493 年提出的。他在自己发表的有关概率统计的专著中提出“如何度量风险？”，后来 Pascal（还记得以他的名字命名的计算机编程语言吗？）和 Fermat 在 1654 年才解决了这个问题。由此可见，风险与不确定性、概率统计等密切相关。但风险这个概念真正开始受到人们的普遍重视并成为现代管理学最“时髦”的用词却是 20 世纪 50 年代之后。

2008 年，国际标准化组织 ISO 风险管理工作组在制定相关标准的时候，在三十余个国家提出的风险定义中采纳了中国专家组提出的关于“风险”的定义，即“**风险是不确定性对目标的影响**”（effect of uncertainty on objectives）。当然，这里所说的风险是最普遍意义上的概念。本书所介绍的风险，则有其自身的特殊内涵。下面就给出什么是**信息安全风险的概念**，除非特殊说明，本书所阐述的风险均是指信息安全风险。



信息安全风险（information security risk），人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件发生及其对组织造成的影响。

这是一个冗长的句子，下面逐一解释，以便读者掌握其深刻内涵。

1．风险和安全

风险和安全是一个矛盾统一体。U.Beck 声称风险社会的驱动力是“我怕”，本质上就是指当一个人感到越不安全的时候，他/她感受到的风险就越高，反之亦然，所以两者是成反比的。这个观点其实与 20 世纪 40 年代美国人本主义心理学家 Abraham Maslow 提出的层次需求理论（Need-hierarchy theory）异曲同工。在这里特别强调的一个观点是风险和安全这对矛盾如何达到某种程度的平衡（统一）？毫无疑问，如果您想达到绝对的安全，最好不要使用任何通信系统，不要使用任何媒介来记录您的秘密，而是把它深深地隐藏在心里（还要假设您晚上睡觉不说梦话）。如果大家都如此效仿，泄露个人秘密的风险肯定是零。但您可能会看到满世界都是和您一样郁郁寡欢的人，而这个世界恐怕也永远不会进步。这个简单的例子实际上说明了一个朴实的真理，人类社会要不断发展，人们就必须不断地在安全防范和承担风险这两方面取得平衡，既要注意安全，又要勇于扛起那些不得不承受的风险。在信息时代，**永远没有绝对的安全和零风险**。人们能

够做的是首先评估风险可能带来的影响，然后采用规避、转嫁和降低风险的方法，最后将风险控制在能够承受的范围之内。这就是风险评估最本质的思想。那么如何将风险控制在能够承受的范围之内呢？需要先做以下铺垫。

2．威胁和脆弱性

在信息安全风险的定义中，**“威胁”**和**“脆弱性”**（也就是人们常说的漏洞）是相辅相成的，前者是产生风险的外因，后者是内因。对于风险的产生，两者缺一不可。例如，一个人不会游泳是其本身的一个弱点（也就是脆弱性），但如果他/她是贝都因人，永远生活在沙哈拉大沙漠中（没有江河的威胁），这个弱点就并不会给其生命带来致命危害。因此仅有脆弱性但无威胁，不会形成风险。反过来，一个防疫人员穿着密封效果很好的防护服（没有漏洞），就不用担心在灭杀细菌（外在威胁）的时候受到感染。所以有威胁但无漏洞，也不会形成风险。这就是中国古话讲的“苍蝇不叮无缝的蛋”的道理。可惜老祖宗讲得过于原则性，没有可操作性。在风险评估工作中，威胁和脆弱性的分析需要遵循一套科学的流程。在接下来的两章中将分别介绍如何识别、刻画信息系统的威胁和脆弱性。

3．组织和资产

“组织”，也就是风险作用的目标（objectives），或者形象地称为“受害者”。在对一个组织机构进行风险评估的时候，如果仅奢谈“组织”可能面临的风险这个抽象的话题，就很难深入下去。例如，泛泛而谈全球气候变暖面临的风险是远远不够的，还需要知道变暖的速度有多快、危害有多大等。为此，就需要分析大气中二氧化碳的含量随着时间增长的曲线、海平面上升一厘米会淹没多少陆地等。所以组织是一个抽象的概念，必须仔细分析组织的结构、功能、属性等，从中抽丝剥茧地分离出若干可以进行定量（至少是半定性半定量）刻画的要素，再运用现代系统科学的理论，也就是定性与定量相结合的方法，形成对风险的理性认识，最后才能凝练出组织可能面临的风险度（高危风险、中度风险、低度风险等）的科学结论。因此，在进行信息安全风险评估中，还需要关注隐藏在上面定义背后的一个关键词，它是一个组织最重要的属性（有时候甚至把它当作组织本身的代名词），它也是各种威胁寻觅的目标，这就是本章最主要的内容，**“资产”**和**“资产价值”**。



随着电子计算机的发明、信息论的提出，特别是 20 世纪 90 年代互联网的飞速发展，使得人与人的交往“更近、更方便”了，但人的不安全感和不信任感也在不断加剧。一方面人们热衷于追捧各种各样的新发明、新创造，同时又对自己创造出来的越来越复杂的虚拟世界感到畏惧，这也许是为什么 U.Beck 的理论风靡一时的原因之一吧。



资产（asset），即对组织具有价值的信息或资源，是安全策略保护的对象。

资产价值（asset value），即资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

在进行信息安全风险评估的时候，首先要明确一个组织机构的资产是什么。例如，在对一家银行进行信息安全风险评估的时候，它的资产是什么呢？当然不是指这家银行金库里的现钞，而应该是这个银行的信息系统及其相关的管理体系（从更宏观的意义上来讲，这个资产比现钞更值钱）。所以本文所涉及的资产是指这个组织的**“信息系统及其管理体系”**。那么如何定性、定量地确认信息系统和管理系统呢？我们将科学地识别一个组织所拥有的信息系统和管理体系的过程称为**“资产识别”**。

4．风险评估和等级保护

现在可以回到“风险和安全”结尾时提出的问题上来了。什么叫做将风险控制在人们可以承受的范围之内？



等级保护与风险评估的关系曾经是学术界探讨的热门话题。两者只取其一行不行？

从法律的角度来讲，国外对信息安全的要求是进行风险评估，如美国的 FISMA 法案，而中国从法律上则要求实施等级保护。因此如何寻找两者之间的结合点是大家关注的话题。此外，风险评估中资产识别、威胁识别和脆弱性识别与等级保护中的系统定级、等级建设和等级维护之间的互动关系也是目前信息安全领域探讨的热门话题。

首先需要对组织的资产进行识别。识别完资产之后，就能明确资产具有什么样的安全需求。如果您只有一元钱，您随身携带就可以了。如果您有一万元呢？您可能会开个普通账户存入银行（这个时候银行就充当了您的保险柜，为您承担风险）。如果您有一亿元呢……因此资产价值的大小决定了安全需求的多少，安全需求决定了必须采取什么样的安全措施（也就是现在大家的流行用语“安全解决方案”）。读到这里，有的读者可能已经把本书前半部分的内容联系起来了。其实安全需求、安全措施结合在一起就是将信息系统按照相应的安全等级保护要求进行建设。换言之，对一个组织所拥有的资产进行识别之后，就能获得该资产的安全保护等级。因此，“等级保护是国家信息安全的基本制度，风险评估是实施等级保护的重要手段”就是这个意思。**资产识别是科学定级的主要依据**。图 7.1 是风险评估和等级保护的关系图。

从图 7.1 可以看出来，当一个信息系统通过了等级验收，进入了日常性的等级运行维护阶段之后，风险就控制在相应的等级之内。换言之，一个信息系统的安全等级相当于这个信息系统能够承受风险的标签。等级越高，防御力度就越大，控制粒度就越细，安全感就越强，风险就越小，但投入也就越大，反之亦然。因此,如何根据一个组织的实际情况进行定级、建设、维护是测评工程师艺术地平衡风险和安全的具体展现。而所有这些工作的基础都是围绕本章的主题——资产识别展开的。

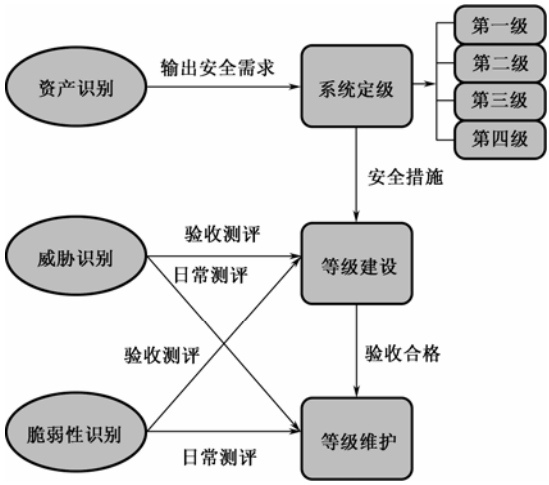


图 7.1　风险评估和等级保护关系示意图

5．风险评估准备工作

在进入本章主题之前，简要介绍一下风险评估工作启动之前所要进行的准备工作。

风险评估的准备工作主要包括以下 6 个方面内容。

1）确定目标

根据组织的业务战略，有关法律、法规和文件精神等，确定此次风险评估的目标是什么。

2）确定范围

风险评估的范围可能是组织全部的信息及与信息处理相关的各类资产、管理机构，也可能是组织所属的一个或几个子机构或子部门。

3）组建团队

风险评估实施团队可大致分为委托评估机构或自评估机构两种形式。关于委托评估机构，在本书第 2 章已经做了介绍。自评估机构则主要是由组织内部的 IT 及其信息安全人员组成。

无论是委托评估还是自评估，风险评估实施团队都必须要有管理层、业务骨干（业务专家，指被评估单位的业务骨干）和信息安全技术骨干组成。

4）系统调研

系统调研的目的是为了对此次风险评估的目标、范围做出初步判断，为撰写风险评估计划做必要的准备。事实上，测评机构进行系统调研可以通过与被测评机构的初步交流来实现。

5）制定方案

根据系统调研所获得的用户的各种资料，测评机构应该向用户提交一份《信息安全风险评估计划》，包括此次评估的目标、范围、依据、技术路线、时间安排、人员安排、保障条件、交付成果等内容。

6）意识培训

向用户事先进行有关信息安全风险评估的意识教育非常必要，它有助于测评人员在风险评估过程中获得用户的理解和支持。

7.2　资产识别的诸方面

本节将介绍在风险评估工作中如何对一个组织的资产进行科学的识别。安全的目的始终都是保障组织业务的正常运行。因此，资产识别的过程就是将组织的业务工作这个抽象的概念逐步分解成定性、定量的资产安全性分析，或者说将组织的业务安全映射成资产的安全，使得我们能够科学地把握组织的业务安全需求及其变化。资产识别包括“**资产分类**”和“**资产赋值**”两个环节。

7.2.1　资产分类

首先要明确，资产的价值不是指信息系统的经济价值，而是与组织的业务工作密切相关。例如，某企业拥有一台高性能服务器，也许价值十余万元，但仅仅被用于该企业的门户网站。而一台普通的 PC 终端存储着该企业的核心技术资料。显然，高性能服务器的资产价值没有这台普通 PC 的资产价值大。

目前国内外关于资产分类的方法较多，大体归纳起来有 2 种，一种是“自然形态”，即按照系统组成成分和服务内容来分类，如分成“数据、软件、硬件、服务、人员、其他”六大类，如表 7.1 所示。

表 7.1　资产分类表

分　类	示　例
数据	保存在信息媒介上的各种数据资源，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册、各类纸质的文档等
软件	系统软件：操作系统、数据库管理系统、软件开发平台等 应用软件：办公软件、数据库软件等 源程序：各种共享源代码、自行或合作开发的各种代码等
硬件	网络设备：路由器、网关、交换机等 计算机设备：大型机、小型机、服务器、工作站、台式计算机、便携式计算机等 存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等 传输介质：光纤、双绞线等 保障设备：UPS、变电设备、空调、保险柜、文件柜、门禁、消防设备等 安全设备：防火墙、入侵检测设备、身份鉴别设备等 其他：打印机、复印机、扫描仪、传真机等
服务	信息服务：该系统对外开展的各种服务 网络服务：各种网络设备、设施提供的网络连接服务 办公服务：为提高效率而开发的管理信息系统，包括各种内部配置管理、文件流转管理等服务
人员	掌握重要形象和核心业务的人员，如主机维护主管、网络维护主管及应用项目经理等
其他	企业形象、客户关系等

这种分类方式的好处是简单、直接、易懂。还有一种资产的分类方法是所谓的“信息形态”，即按照信息论、系统论的观点，将资产分为“信息、信息载体和信息环境”三大类，如图 7.2 所示。

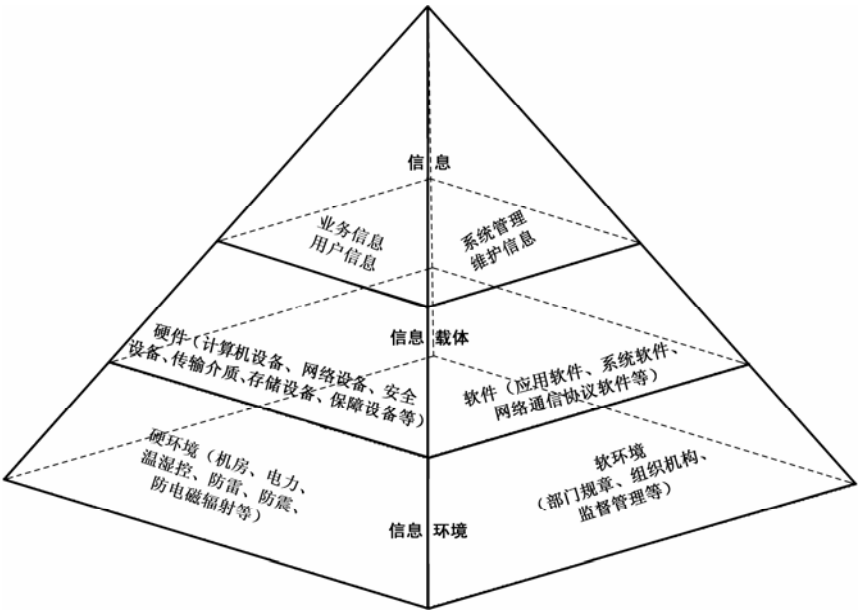


图 7.2　资产分类示意图

对资产进行分类，不是简单的“对账”，统计有多少网络设备、安全设备、服务器和 PC 终端等，而是要和该组织的工作职能、业务范围、发展战略等挂起钩来，中国 IT 界常用一个舶来品名词“**业务战略**”（business strategies）来称谓它（其实西方人谈论战略的时候最推崇的是中国的孙子）。要提醒读者注意的是，将业务战略与资产进行关联是风险评估工作中的重中之重，也是一个难点。在后面将结合具体案例和读者一起探讨如何逐步将组织的业务战略映射到组织的资产乃至整个风险评估之中。

无论是采用“自然形态”还是“信息形态”的分类方式，均必须将组织的资产与组织的业务战略映射起来。本书将采用“信息形态”这种分类方式。表 7.2 是“信息形态”分类指导表，谨供参考。

表 7.2　“信息形态”分类指导表

分　类			示　例	对应体系
信息及信息载体	专属信息及信息载体	信息（数据）资产	业务信息：如客户信息、交易信息等 用户信息：如内网各种设备口令、账户等 系统管理信息：如内网安全审计日志、IP 地址、VLAN 划分、设备配置信息等	技术体系
		应用资产	如子系统专属的应用系统及相关软件	
		系统资产	如操作系统、数据库系统等系统软件	
		硬件资产	如子系统专属服务器及相关硬件设备	

续表

分类			示例	对应体系
信息及信息载体	公共信息及信息载体	信息（数据）资产	业务信息：如企业形象、业务介绍等 用户信息：如外网及门户网站口令、账户等 系统管理信息：如外网及门户网站日志、IP 地址、设备配置信息等	技术体系
		应用资产	如应用协议及软件	
		系统资产	如操作系统、数据库系统等系统软件	
		网络资产	如网络协议、通信协议	
		硬件资产	如终端设备、网络通信设备、安全防护设备、传输介质、存储介质	
信息环境		硬环境	如机房、电力、照明、温控、湿控、防盗、防火、防震、防水、防雷、防电磁辐射、抗电磁干扰等设施	
		软环境	如国家法律、行政法规、部门规章、政治经济、社会文化、思想意识、教育培训、人员素质、组织机构、监督管理、安全认证等方面	管理体系

在 7.3 节“资产识别案例分析”中将基于这个分类指导表来逐步细化信息、信息载体和信息环境，使之与被评估单位的业务战略相对应。下面先就资产与业务战略的映射方法做一个介绍。



从事过软件研发工作的读者可能都知道，在开发一个应用软件的时候，最困难的环节是“需求调研”，因为它必须和用户的业务工作联系起来。资产识别过程中如何将资产与业务战略对应起来也是如此。民政部门与检察院的业务战略就完全不同，金融保险行业与汽车电子生产企业也大相径庭，尽管它们的信息系统里所配置的设备可能都相差不多。以下是作者根据工作经验给读者的建议，使得一个“外行”的信息安全风险评估人员能够逐步了解一个被评估单位的业务战略，我们称为“一读二问三查看”。

（1）**阅读**：获得并仔细分析被评估单位信息化建设的有关文档，如《信息化发展战略规划》、《信息化建设实施计划》、《信息化建设实施方案》等。任何一个单位信息系统的建设都是以进一步提升其业务发展为目的的。在这些文档中，风险评估人员可以获得该单位的战略规划、建设目标、组织机构、实施步骤、现有规模、资金投入等大量翔实的资料。进而凝练出被评估单位的业务战略（读者将会在 7.3 节案例分析中看到这样的例子）。

（2）**询问**：与被评估单位分管信息化建设的领导、信息中心的领导和工作人员交流。尽管一个组织的业务战略可以通过查阅该组织的各种信息化建设资料获得一个大致轮廓。但作为该单位信息化建设组织实施和运行服务的枢纽，信息中心的领导及其工作人员对该组织业务战略有更深刻的把握。他们是整个风险评估工作中的“领域专家”（domain experts），既了解本单位的业务发展战略，又清楚本单位信息化发展现状。事实上，风险评估中的自评估队伍就是以该单位信息中心的人员为主组成的。

（3）**查看**：到被评估单位各个业务部门实地考察信息系统的应用情况。仅仅通过阅

读和交流还不能对一个组织信息化应用的现状有一个完整和真实的了解。风险评估人员应当尽可能地到该组织的各个业务部门具体查看信息化应用情况，从而对组织的业务战略的实施情况有一个亲身的体会。

相信读完了本书上半部分的读者已经总结出来了，资产识别的方法与安全测评中的“现场调研”是非常类似的，只不过资产识别的现场调研更关注被评估单位的业务战略，安全测评则是根据国家有关标准进行细节的核对。通过这些访谈调研，评估人员对该单位的业务战略就有了一个全面的了解。接下来就需要将“业务战略”映射到“资产”。为此建议：

（1）被评估单位需向评估人员提供信息系统的各种软、硬件资料，网络承建商和软件供应商的相关资料及信息系统有关的各类管理体系文档等。例如，软件供应商为组织撰写的各种应用软件开发文档资料可以使得评估人员进一步了解该组织的业务战略是如何体现在各种应用软件系统里面的；系统集成商是否有相应的集成资质（从而也表明了该组织在遭遇事故的时候转嫁风险的渠道）等。

（2）根据上面所了解到的实际情况，对被评估单位中心机房等要害部门进行实地调研，考察机房环境，核对网络拓扑，比对核心网络设备、各种服务器（数据库、Web、邮件、应用等）及安全设备的型号、版本等信息。在征得被评估单位允许的前提下，也可以使用数码相机等对各种设备和机房环境进行拍照，以便在撰写资产识别报告的时候核对各种信息和对资产进行精确的分类。

根据上述获得的资料及对组织业务战略的分析，就能够将抽象的业务战略与具体的资产逐步捆绑起来。举例而言，一家信息化程度很高的汽车生产企业，在激烈的市场竞争中不断推陈出新是其主要的业务战略，其核心资产毫无疑问就应该包括（但不仅限于）该企业汽车设计研究院的各种数字化设计资料（如新款汽车的各种参数资料）、生产工艺资料及严格的技术资料使用管理制度等；而政府税务部门的业务战略（工作职责）则是进行各种税种的征收和管理，因此其核心资产就应包括（但不限于）纳税人数据库服务器、大型应用软件（如用于网上申报税收信息的应用软件）等。

尽管由于被评估单位业务战略千差万别，不可能在本书中一一列举，但在进行资产识别的时候，还是有一套科学的识别方法来“提纲契领”，这就是始终抓住信息安全的本质属性来进行资产分类。“保密性”、“完整性”和“可用性”是信息安全最基本的三个属性。在对资产进行分类的时候，实际上就是结合组织的业务战略，并根据信息安全的这三个属性来一一评判每个资产的。例如，在上面“信息形态”分类方式中，可以结合信息安全的这三个属性，对数据、软件、设备等进行以下更加详细的分类，如表 7.3 所示。

表 7.3　根据安全属性对信息资产进行分类

分　类	示　例			
业务数据 A	保密性	完整性	可用性	应用部门/人员
	业务数据 A 是否有保密性要求 □有 □ 无	完整性要求描述	可用性要求描述	使用数据 A 的部门/人员清单

续表

分　类	示　例			
专用软件 A	软件 A 是否有保密性要求 □有 □ 无	完整性要求描述	可用性要求描述	使用软件 A 的部门/人员清单
设备 A	设备 A 是否有保密性要求 □有 □ 无	完整性要求描述	可用性要求描述	使用设备 A 的部门/人员清单



一般而言，不是每种业务数据都有保密性要求。例如，政府部门的门户网站数据都是公开的，但每一种数据都有完整性和可用性要求，只不过粒度不同，如可用性就可以分为实时可用和恢复后可用等。软件保密性是指本单位拥有知识产权的软件等。如果是外包开发的软件项目，则需根据相关合同来界定。设备的保密性要求也是根据组织的业务战略来确定的。例如，政府部门对涉密用计算机有专门的要求。企事业单位也应根据自己工作的性质和业务需求来决定哪些设备需要保密。

图 7.3 是资产分类的流程图。

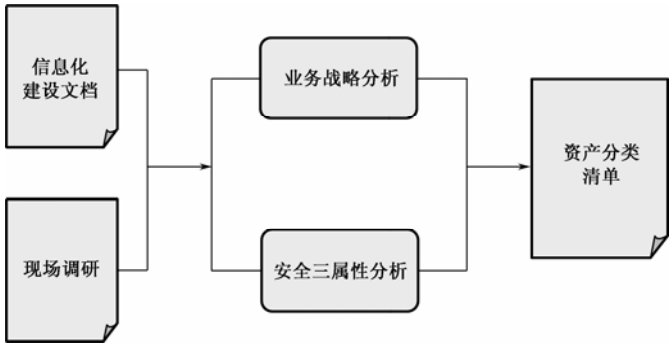


图 7.3　资产分类流程图

7.2.2　资产赋值

当声称一个组织的资产价值很高的时候，依据是什么呢？在资产分类的基础上，进一步对资产进行半定性半定量的分析，即进行资产赋值，从而对组织的资产价值有一个科学理性的认识。资产首先被分解成更详细的“保密性赋值”、“完整性赋值”和“可用性赋值”三个安全属性赋值，然后在这个基础上又综合分析得出资产重要性等级。



目前大多数国家（包括中国）在自然灾害和人为重大安全事故等公共事件预警和响应方面，往往采用“四级分级制”，即“红色预警/I 级响应”、“橙色预警/II 级响应”、“黄色预警/III 级响应”和“蓝色预警/IV 级响应”，分别代表风险的严重程度和相应的处置级别。将信息安全风险的级别与公共安全风险的级别融合在一起，是目前信息安全风险研究值得关注的方向。

1．资产安全性赋值

为了使得不同安全属性的资产赋值具有归一性，国家标准统一采用了“5 级分级制”（这正好又与等级保护的 5 个级别遥相呼应）。即“很高”、“高”、“中等”、“低”和“很低”。表 7.4、表 7.5 和表 7.6 是关于资产保密性、完整性和可用性的赋值表。

表 7.4　资产保密性赋值表

赋　值	标　识	定　义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成对组织的灾难性损害（如企业的核心技术秘密、电子政务内网中传递的国家秘密等）
4	高	包含组织的重要秘密，其泄露会使得组织的安全和利益遭受严重损害（如科研单位正在组织研发的项目信息）
3	中等	组织的一般性秘密，其泄露会使得组织的安全和利益受到损害（如企业正在酝酿但尚未出台的职工福利政策）
2	低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害（如某企业内部人员出勤率）
1	很低	可对社会公开的信息，公用的信息处理设备和系统资源等（如政府和企事业单位的门户网站）
备注：具体的赋值情况应由风险评估人员和被评估单位人员共同确定		

表 7.5　资产完整性赋值表

赋　值	标　识	定　义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补（如上市公司的年度经营报表）
4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补（如某企业的项目投资计划）
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但可以弥补（如企业对核心技术人员的岗位补贴）
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微的影响，对业务冲击轻微，容易弥补（如网上购物的品种信息）
1	很低	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略（如某企业已经废弃的车间改造计划方案）
备注：具体的赋值情况应由风险评估人员和被评估单位人员共同确定		

表 7.6　资产可用性赋值表

赋　值	标　识	定　义
5	很高	可用性价值非常高，合法使用者对信息及其信息的可用度达到年度 99.9%以上，或系统不运行中断（如证券交易中心的数据和核心交换机）
4	高	可用性价值非常高，合法使用者对信息及其信息的可用度达到每天 90%以上，或系统允许中断时间小于 10min（如医院信息系统的门诊挂号分系统）

续表

赋　值	标　识	定　义
3	中等	可用性价值中等，合法使用者对信息及其信息的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30min（如地区政府门户网站的 Web 服务器）
2	低	可用性价值较低，合法使用者对信息及其信息的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60min（如高校英语四、六级考试成绩在线通知）
1	很低	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%（如建成光纤通信局域网后企业使用的 MODEM 拨号上网系统）
备注：具体的赋值情况应由风险评估人员和被评估单位人员共同确定		

2．资产重要性等级

资产识别工作的最后一步是资产重要性等级赋值，也就是通常所说的资产价值。资产价值是对资产保密性、完整性和可用性的综合评定。综合评定方法有两种：

（1）根据保密性、完整性或可用性赋值中最高的取值来代表该资产重要性等级。

（2）对保密性、完整性和可用性赋值进行加权平均的方式来决定该资产的重要性等级。

上述两种方法没有优劣之分，而是应该根据被评估单位的实际情况来决定。表 7.7 给出了资产等级及其具体含义。

表 7.7　资产等级表

赋　值	标　识	定　义
5	很高	非常重要，其安全属性破坏后可能对组织造成非常严重的损失
4	高	重要，其安全属性破坏后可能对组织造成比较严重的损失
3	中等	比较重要，其安全属性破坏后可能对组织造成中等程度的损失
2	低	不太重要，其安全属性破坏后可能对组织造成较低的损失
1	很低	不重要，其安全属性破坏后对组织造成很小的损失，甚至忽略不计
备注：具体的赋值情况应由风险评估人员和被评估单位人员共同确定		

从上面的资产重要性等级分类可以看出，它和信息系统安全等级保护定级要求是一脉相承的（参见本书前半部分），这就是为什么说风险评估是等级保护的主要手段的含义。



至此就完成了“业务战略→资产识别→资产分类→资产安全性赋值→资产重要性赋值→对组织业务战略相关的安全认识”的螺旋上升的分析历程。换言之，我们完成了一个从“定性→半定性半定量→定量（如果可能的话）→更准确的定性”这样一个系统的、科学的资产识别过程。作者在这里发挥自己笨拙的想象力，不妨把这个过程称为“礼花模型”（见图 7.4）：在 2008 年北京奥运会开幕式上，当一枚礼花弹从“鸟巢”升腾而起的时候，人们看见的是一道逐步扩散的闪亮的轨迹，然后每个轨迹又散发成诸多细小的分枝，接下来每一个分枝又爆发出若干朵绚丽夺目的礼花……

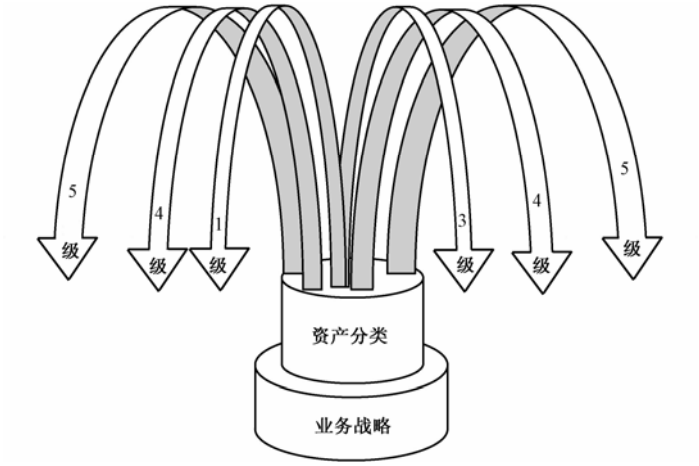


图 7.4　资产分类“礼花”模型

7.3　资产识别案例分析

从本节开始，将以某大型企业为例，介绍信息安全风险评估工作中的资产识别、威胁识别、脆弱性识别和风险分析等各个环节。本节将介绍资产识别过程及该过程结束后应该输出的技术报告。承担此次风险评估工作的是本书前半部分虚拟的专业测评机构——“深海”信息安全测评中心。

7.3.1　模拟案例背景简介

1．企业背景

兰曦电子科技（集团）有限公司（如图 7.5 所示，以下简称“兰曦公司”）隶属中国电子工业集团，始建于 20 世纪 70 年代“三线建设”时期，是巴山市大型骨干企业。兰曦公司下辖 12 个分公司、1 个研究院，固定资产 18 亿元，行业职工 8 千人，研发和生产各种精密电子设备和元器件，年销售收入 120 亿元，税利 15 亿元，业务范围涉及“技、工、贸”等多个领域。“十五”期间，公司在中国电子工业集团和巴山市政府的指导下，积极贯彻 “以信息化带动工业化、以工业化促进信息化”的发展方针，高度重视行业信息化建设，初步实现了“数字兰曦”目标，提高了行业整体竞争实力。



图 7.5　兰曦电子科技（集团）公司

2．业务战略

“以管理创新为基础，以业务应用为主导，以信息资源共享为核心，以数据中心为

支撑，以提高行业整体竞争力为目的，建成功能完善、高效实用、高度集成、具有国内先进水平的“数字兰曦”，促进行业可持续发展”——摘自“兰曦”公司《十一五信息化发展规划》。



对于初次接触信息安全风险评估的读者来讲，不仅要熟悉信息安全领域的技术细节和术语，还要耐心学习不同组织的“行业用语”，善于从被评估单位的业务战略中提取出与信息化建设相关的内容，从而为下一步进行**基于业务战略的资产识别**打下基础。要牢牢记住任何一个组织不惜花费重金打造现代化的信息系统，其目的始终都是为了提高该组织的管理水平，从而获得更高层次的生产或服务效率。因此，读者应从这个角度来体会以下兰曦公司信息化目标的“四力”，经验丰富的读者其实也可以看出这“四力”实际上具有普适性。

3．信息化目标

“推进管理量化能力；实现快速响应能力；提升科学决策能力；增强整体竞争实力”——摘自《“数字兰曦”建设纲要》。

信息化建设是一个复杂的系统工程，需要一个组织机构从领导决策层面、管理层面和操作层面配备充足的管理和技术资源。

4．信息化组织机构

“兰曦公司信息化组织机构健全，职责明确，管理规范。公司信息化领导小组负责“数字兰曦”信息化建设决策等工作；公司信息中心具体负责全公司信息化建设和“数字兰曦”中心机房运行维护工作；下属各单位信息部门负责系统应用维护等工作。全公司信息系统管理和运行维护从业人员 211 人，本科以上专业技术人员 108 人；人均拥有计算机覆盖率达 83%；制定了行业信息化管理、网络建设、信息安全、系统应用等方面的规章制度、规范性文件 29 份，其中，规划类 3 份，管理类 17 份，公司内部技术标准类 4 份，工作要求类 15 份。形成一套较为完整的信息化管理体系。”——摘自《“数字兰曦”建设纲要》。

下面将对兰曦公司信息化建设的概况做一个简介，使得读者在进行资产识别之前，对兰曦公司的信息化“总资产”有一个概要性的认识。

5．信息化建设概况

从 2000 年至今，“兰曦”公司先后投入信息化建设资金 1.5 亿元，建成了“决策支持”、“电子政务”、“电子商务”、“生产管理”、“运行保障”五大业务系统，在 2008 年实现了“数字兰曦”目标。“数字兰曦”信息系统包括一个网络平台、一个行业数据中心，电子政务、电子商务、辅助决策三大应用系统共 16 个信息系统，覆盖全公司 12 个分公司、1 个研究院和全国 145 个销售网点。

从逻辑上来讲（见图 7.6），“数字兰曦”包括 3 个层面，即基础层、应用层和决策

层。基础层主要包括组织的网络基础设施建设，是信息化建设的初级阶段；应用层是目前各个单位信息化建设的主体，代表着一个组织是“重建设、轻应用”还是真正开始发挥信息系统对业务发展的杠杆作用，是信息化建设的成熟阶段；决策层是信息化建设的高级阶段，使用对象是一个组织的领导层。例如，兰曦公司的管理者需要从“数字兰曦”中获取各种经过统计分析的数据，并在决策层的各种智能分析软件的协助下进行决策活动。

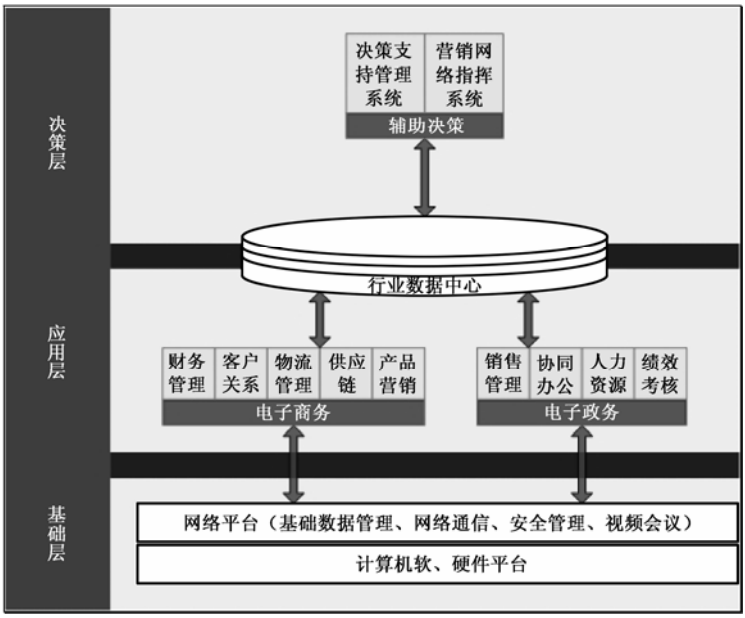


图 7.6　“数字兰曦”系统框架图

在对“数字兰曦”有了大致了解之后，下面进入本节的主要内容，对“数字兰曦”进行资产分类和资产赋值。

7.3.2　资产分类

如本章前面所述，广义上的资产是指对单位具有价值的任何东西。在风险评估过程中，首先要明确评估对象的边界和范围。本案例中的资产是指**与“数字兰曦”相关联的**，由兰曦公司赋予了价值因而需要保护的东西。它可能是以多种形式存在，包括无形的、有形的、硬件、软件、文档、代码、服务、企业形象等。

在风险评估中关注的是资产的安全性。信息系统资产的保密性、完整性和可用性三个安全属性反映了资产的安全特性。信息资产安全特性的不同也决定了其信息价值（资产的重要程度和敏感程度）的不同，因此资产面临的威胁、存在的脆弱性、需要进行的保护和安全控制措施都各不相同。同时，资产还具有很强的时间特性和系统属性，它的价值和安全属性都会随着时间的推移及系统的变化而发生变化，所以应该根据时间变化的频度和系统的变化制定资产相关的评估和安全策略的频度。本案例中的“数字兰曦”

属于已经建成的信息系统，各种资产的安全属性相对稳定。下面采用本章前面所介绍的“信息形态”分类法，对“数字兰曦”的资产进行分类。

1．信息环境资产

兰曦公司在信息系统的规划、建设、运营过程中建立了较为完善的信息化管理体系，并利用所建立的体系对企业的信息化建设和运行维护进行了有效的管理和指导。然而，在本次风险评估的调研和资料分析过程中，测评人员发现“数字兰曦”出现过系统断电、病毒入侵、人员恶意篡改数据等安全事件，这也说明了“数字兰曦”管理体系在信息安全保障工作方面存在一定的不足（详见后面两章“威胁识别”和“脆弱性识别”）。

信息环境资产包括软环境资产（组织机构资产、管理制度资产等）和硬环境资产（信息中心机房资产）。

1）组织机构资产

“数字兰曦”管理体系的组织结构依据整个系统的区域分布划分为总公司信息化领导小组、总公司信息中心、分公司信息科/部 3 个层次。**总公司信息化领导小组**负责研究制定全公司信息化建设方针、政策决策，审定全公司信息化建设规划，协调解决信息化建设中的重大问题，对信息化建设资金的使用进行监管。**总公司信息中心**（以下简称信息中心）负责拟订“数字兰曦”信息化发展规划和规章制度，审核“数字兰曦”网络平台、数据中心、电子政务体系、电子商务体系、管理决策体系的建设、推广、管理和培训、应用维护，负责本公司各个业务部门固定资产信息的统计、汇总、分析、培训工作，编制分析报告；负责公司机关计算机设备相关固定资产的管理、维护。**分公司信息科/部**负责本部门信息系统应用维护工作。兰曦公司组织结构如图 7.7 所示。

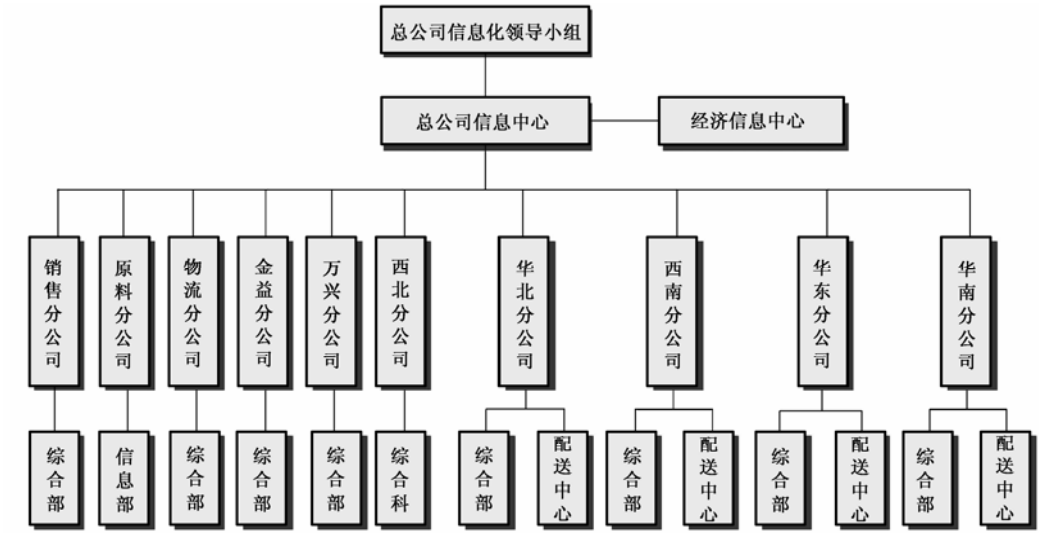


图 7.7　兰曦公司组织结构图

尽管兰曦公司业务应用较为复杂，涉及单位和部门众多，但由于“数字兰曦”对大部分业务实现了业务大集中和数据大集中的模式，其重要信息化管理人员主要配置在公司信息中心，因此，信息中心代表了兰曦公司组织机构的核心资产。信息中心的组织机构资产包括“岗位”和“人员”两部分，如表 7.8 所示。

表 7.8　“兰曦公司”信息中心岗位资产

岗 位 设 置	岗 位 职 责
信息中心 主任岗	① 负责本部门业务、行政及思想政治工作 ② 负责组织编制全公司信息化工作中长期发展规划和年度实施计划并组织实施 ③ 负责对全公司行业信息化工作进行管理、指导和检查 ④ 负责组织实施全公司信息化工程项目的立项、验收和信息化成果的鉴定、技术推广、标准规范工作 ⑤ 负责公司卫星网络、广域网和局域网的建设、管理和应用维护，负责信息安全系统的建设、管理和应用 ⑥ 负责公司电子政务系统（包括门户网站）的建设、管理和应用维护 ⑦ 负责公司信息资源的管理和规划，负责数据中心及辅助决策支持系统的建设、管理和应用维护 ⑧ 完成公司信息化领导小组交办的其他事宜
信息中心副主任岗	① 协助负责本部门业务、行政及思想政治工作 ② 协助负责公司信息化工作管理、指导和检查 ③ 负责“数字兰曦”电子商务信息系统的建设、管理和应用 ④ 负责公司机关计算机设备相关固定资产的管理、维护，负责公司信息中心机房的管理和运行 ⑤ 组织和建设全公司信息化工作队伍，开展相关的各类业务和技术培训 ⑥ 完成公司领导和信息中心主任交办的其他事宜
行业信息化 管理岗	① 做好公司信息化建设和计算机应用的技术组织和指导工作 ② 参与编制公司信息化工作和“数字兰曦”应用的中、长期发展规划 ③ 拟定公司信息管理的有关规章制度，负责公司信息化建设项目的日常管理工作 ④ 对公司信息化工作（包括技术培训）履行管理、指导职能，组织实施公司信息化工程项目的立项、验收等工作 ⑤ 完成主任交办的其他工作
电子商务 管理岗	① 负责“数字兰曦”电子商务系统的建设、管理和运行维护 ② 负责拟定电子商务信息系统有关规章制度 ③ 负责电子商务信息系统相关设备的管理 ④ 完成主任交办的其他工作
电子政务 管理岗	① 负责“数字兰曦”门户网站的建设、管理和应用维护 ② 负责公司办公自动化的建设和维护 ③ 负责制定电子政务相关规章制度 ④ 完成领导交办的其他工作
信息资源 管理岗	① 负责拟定公司信息资源相关规章制度 ② 负责电子行业信息的采集、汇总、分析和预测工作 ③ 负责电子行业信息资源的管理和规划，负责信息代码日常维护 ④ 负责电子行业数据中心和决策支持系统的建设、管理和应用维护 ⑤ 完成领导交办的其他工作

续表

岗 位 设 置	岗 位 职 责
网络维护及安全管理岗	① 负责机关局域网、广域网的规划、建设、管理和应用维护 ② 负责公司地面骨干网（到中国电子工业集团）的建设和维护 ③ 负责规划机关综合布线，指导行业各单位综合布线工程 ④ 负责公司及下属分公司、研究院信息安全系统的规划、建设和管理维护 ⑤ 负责公司各单位视频会议系统的建设、管理和使用 ⑥ 完成领导交办的其他工作
设备维护及机房管理岗	① 负责公司机关计算机设备的管理、维护 ② 负责公司中心机房的管理和运行维护 ③ 负责机关信息化固定资产管理 ④ 负责部门内部日常事务处理 ⑤ 完成领导交办的其他工作

读者可以将兰曦公司信息中心岗位设置与公司业务战略进行对比，从而体会这些岗位是如何贯彻“以管理创新为基础，以业务应用为主导，以信息资源共享为核心，以数据中心为支撑……”这一业务战略思想的。

在对人员资产进行分类的时候，要特别重视关键岗位的人员所接受的专业培训，如“首席信息主管”（CIO）、“首席信息安全主管”（CISO）等方面的培训。同时要注意相关人员的任职年限，从表 7.9 所示的数据中可以看出从业人员对本单位信息系统的熟悉程度。

表 7.9　“兰曦公司”信息中心人员及履历资产

姓　　名	工 作 类 型	受过何种 IT 培训	培训的频度	职　　务	任现职年限
袁前	主持信息中心工作	高级 CIO 培训	1 次	主任	4 年
高山	系统安全 网络管理	中级 CIO 培训 CISO CCNA 培训 计算机信息安全管理培训	4 次	副主任	4 年
许三	设备维护及机房管理	中级 CIO 培训 计算机网络管理培训	各 1 次	主任科员	4 年
成今	系统管理 电子商务管理	中级 CIO 培训 IBM DB2 培训	各 1 次	主任科员	3 年
史明	电子政务管理	中级 CIO 培训	1 次	主任科员	3 年
伍东	“兰芯”子系统管理	中级 CIO 培训 计算机网络管理培训	各 1 次	副主任 科员	1 年



细心的读者可能已经发现上述信息中心的“岗位”和“人员”资产清单没有完全一一对应。事实上，每个组织在拟定岗位职责的时候，均是根据本单位的长远发展战略

目标来确定的，因此具有普适性和通用性，其内容也是相对静态不变的。在具体工作中则会根据信息系统的不同发展阶段来分配各个工作人员的业务管理内容，所以是动态变化的。例如，上面的“兰芯”子系统就是“数字兰曦”刚建成的一个核心子系统（见下面专用信息及信息载体资产识别），所以需要专人（如伍东）管理。

2）管理制度资产

管理制度资产不仅仅是简单统计一个组织有多少管理制度和文档，而是应当对这些管理制度的实施情况给予一个总结。下面就是本案例中对兰曦公司的相关管理制度的概述。

在“数字兰曦”的运行维护过程中，兰曦公司制定了行业信息化管理、网络建设、信息安全、系统应用等方面的规章制度、规范性文件 29 份。其中，规划类 3 份，管理类 17 份，技术标准类 4 份，工作要求类 15 份。形成了一套较完整的信息化管理规章制度。

在上述规章制度中，应用较为广泛和成熟的文档包括《中心机房管理办法》、《公司视频会议系统运行管理办法》、《“数字兰曦”网络建设及管理规范》、《“数字兰曦”网络安全管理办法》、《中国电子工业集团关于加强行业互联网管理工作的通知》、《中国电子工业集团兰曦电子科技（集团）公司——关于加强计算机信息系统安全管理的通知》。其中《中心机房管理办法》对进出机房的访问控制、机房环境的监控、机房内重要设备的访问控制进行了指导性的规定，但缺少更细粒度的操作规范说明；《“数字兰曦”网络建设及管理规范》提出了“数字兰曦”网络建设的原则和目标，对建设行业各级专网的技术要求进行了规范，并对公司及其下属单位进行了统一的 IP 地址分配，是“数字兰曦”建设的一个规范性的指导文档；《“数字兰曦”网络安全管理办法》对兰曦公司的内部工作人员使用、配置计算机和网络设备制定了统一的操作要求，但是缺少细粒度的技术要求（如密码设置的规则）和相应的监控管理办法；《中国电子工业集团兰曦电子科技（集团）公司——关于加强计算机信息系统安全管理的通知》对公司各部门接入互联网的办法进行了规定，但对已接入互联网的部门缺少其对互联网访问控制的具体管理规定。

从上面对管理制度资产的概述中可以看出，评估人员不是简单地统计一个组织有多少份管理文件，而是将这些管理文件中与信息安全三个属性有关的内容提取出来，并根据实际执行情况给予一个总体评价。

表 7.10 将公司有关“数字兰曦”的管理制度及相关部门/人员进行了关联，有利于在进行管理制度资产识别中分清责任关系，并在评估结束后需要对管理制度进行持续改进的时候，将需要进行整改的管理文档落实到具体部门或责任人。

3）信息中心机房资产

“数字兰曦”中心机房是整个信息系统的运行基础和最基本保障。为了保证全行业系统的正常运行，兰曦公司在《“数字兰曦”网络建设及管理规范》文档中对全公司各级机房的建设标准进行了统一的要求：新建机房和改造旧机房必须严格按照国家计算机机

房建设标准进行，公司中心机房应达到国家 A 级以上标准，分公司机房应达到国家 B 级标准（有兴趣的读者可以查阅国家关于计算机机房建设的国家标准），如表 7.11 所示。

表 7.10　“数字兰曦”管理制度资产

组 织 机 构	人 员 配 置	管 理 制 度	
公司信息化领导小组	李龙	规范性管理制度文件共 29 份：规划类 3 份，管理类 17 份，技术标准类 4 份，工作要求类 15 份	《中心机房管理办法》
	赵刚		
	袁前		
	高山		
公司信息中心	袁前		《中国电子工业集团关于加强行业互联网管理工作的通知》
	高山		
	许三		
	成今		
	史明		《中国电子工业集团兰曦电子科技（集团）公司——关于加强计算机信息系统安全管理的通知》
	伍东		
……			

表 7.11　“数字兰曦”中心机房资产

名　　称		生 产 厂 家	类型/规格	数　量	备　　注
设施	防火设施	深圳云涛	七氟丙烷	1 台	
	门禁设施	北京门吉利	感应卡式	1 台	
	防雷接地设施	德国 LEUTRON	2 组三相，25 组单相	27 组	接地装置
	防渗漏措施				空调下有漏水检测装置
	绝缘地板	沈飞	600cm×600cm		抗静电地板
设备	UPS 电源	美国 APC	APC InfraStruXure		功率：30 kVA+1
	空　调	英国 DENCO D42MAH		2 台	
	机　柜	订做	200cm×60cm×30cm	6 台	
		IBM	170cm×60cm×30cm	4 台	
		IBM	160cm×60cm×60cm	4 台	
	摄像机	Shepherd	半球状	4 台	覆盖率：80%
	报警器		声光报警器	4 个	覆盖率：90%
	火警监控器	12 个烟感	8 个温感	20 个	覆盖率：90%

以上对“数字兰曦”的信息环境资产进行了分类。接下来将对“数字兰曦”的公用信息载体资产进行分类识别。

2．公用信息载体资产

公用信息载体资产是指整个信息系统的基础网络平台，但不包括信息系统各子系统的专用设备（见下面“兰芯”子系统）。公用信息载体资产为整个信息系统的信息提供传输通道，对信息进行安全检查并对其流向进行控制，同时也对信息进行最初始的采集、加工和最后的处理、应用；涉及到信息系统信息的采集、处理、传输、存储、应用

的各个环节，因此保障公用信息载体资产不被非法访问和破坏是保障整个信息系统安全和最终的信息安全的关键点之一。

在对公用信息载体资产进行识别的时候，要注意被测评单位所提供的网络拓扑图与实际情况是否相吻合。由于网络拓扑图往往是系统承建商在建设初期所绘制的，随着信息系统的不断演化，实际情况可能会有所变化。因此，建议测评人员要进行网络布线的现场调研，并与所获得的网络拓扑图进行对比。

“数字兰曦”现有基础网络平台是在 1998 年建成的公司总部与所属 13 个单位之间的广域网的基础上建立的，采用了 2M SDH 和 1M FR 的链路冗余备份，主干通信设备也进行了双机热备，关键节点设置了防火墙和基于网络和主机的 IDS，并为全公司 4500 余台终端设备设置了统一的防病毒系统，在 2004 年还建立了包括全公司 44 个下属单位的视频会议系统。图 7.8 是“数字兰曦”网络拓扑简图。

在公用信息载体资产中，又可以分解为“通信载体资产”（见表 7.12）和“安全防护资产”（见表 7.13）两个子类（这种分类方式不是唯一的，读者可根据自身情况予以细分）。请读者注意，为了明确各种资产的管理责任我们将这些设备资产与使用部门进行了关联。例如，核心交换机 CISCO6506 等是属于整个“数字兰曦”基础通信网络的一部分，所以所属部门为“数字兰曦”；楼层交换机 CISCO3550 主要用于兰曦公司总部，由兰曦公司信息中心负责管理，所以所属部门为“信息中心”；交换机 QuidWay S6506R 是“数字兰曦”的核心子系统“兰芯”所使用的，因此所属部门为“兰芯”子系统（见下面“专属信息及信息载体资产”），等等。

表 7.12　通信载体资产

序号	名　称	型　号	数　量	生产厂家	使用年限	网络操作系统版本	资产编号	所属系统
1	核心交换机	CISCO 6506	1 台	CISCO	5 年	s3223_rp-IPBASE_WAN-M	X_A01	“数字兰曦”
2	核心交换机	CISCO 4506	1 台	CISCO	2 年	cat4000-I5S-M	X_A02	“数字兰曦”
3	楼层交换机	CISCO 3550 系列	10 台	CISCO	5 年	—	X_A03	信息中心
4	交换机	s5126	1 台（kM）	华为 3COM	2 年		X_A04	信息中心
5	交换机（物流公司）	QuidWay S6506R	1 台	华为 3COM	1 年	S6506R-3032	X_A05	“兰芯”子系统
6	交换机（研究院）	QuidWay S3952P/S3928P	6 台	华为 3COM	1 年	VRP 3.10	X_A06	研究院楼层交换
7	交换机（分公司）	QuidWay S3928P	1 个分公司 1 台	华为 3COM	1 年	VRP 3.10	X_A07	分公司机房
8	核心路由器	QuidWay NE20（OSPF 路由协议）	1 台	华为 3COM	1 年	VRP 5.10	X_A08	连接下属各分公司

续表

序号	名　　称	型　　号	数　　量	生产厂家	使用年限	网络操作系统版本	资产编号	所属系统
9	核心路由器	CISCO 7206（OSPF 路由协议）	1 台	CISCO	7 年	C7200-JS-M 12.2	X_A09	连接下属各分公司
10	路由器（连接巴山市商业银行）	CISCO 3745（静态路由）	1 台	CISCO	2 年	C3745-IPBASE-M	X_A10	“兰芯”子系统
11	路由器（连接中国电子工业集团）	CISCO 3825（BGP 路由协议）	—	CISCO	2 年	—	X_A11	信息中心
12	分公司路由器	QuidWay AR4640（OSPF 路由协议）	40 台	华为 3COM	1 年	VRP 3.40	X_A12	分公司机房
13	分公司路由器	CISCO 2600（OSPF 路由协议）	42 台	CISCO	4～6 年	C2600-I-M 11.3	X_A13	分公司机房
	……							

表 7.13　安全防护资产

序号	名称	型　　号	数量	生 产 厂 家	使用年限	网络操作系统版本	资产编号	所属系统
1	互联网防火墙	4000V2	2 台	天融信	4 年	V3.21	X_FH01	信息中心
2	广域网防火墙	FortiGate 1000A	1 台	FORTIGATE（美国）	1 年	FGT1KA-3.00-FW-build468-061213	X_FH02	连接分公司
3	分公司防火墙	POWER-V 404	36 台	联想网御	1～3 年	PF500	X_FH03	连接分公司
4	分公司防火墙	NETPOWER	4 台	北京中科网威	—	V3.21	X_FH04	连接分公司
5	“冰之眼”入侵检测	1600D	1 台	中联绿盟	4 年	暂缺	X_FH05	信息中心
6	“天眼”入侵检测	NPIDS-100	1 台	北京中科网威	4 年	暂缺	X_FH06	信息中心
7	主机入侵检测系统	QuidWay S3928P	1 台	Symantec	4 年	暂缺	X_FH07	信息中心
8	“极光”漏洞扫描	“极光 V4”	1 台	中联绿盟	4 年	暂缺	X_FH09	信息中心
	……							

1）通信载体资产

通信载体资产既包括兰曦公司中心机房的网络通信设备，也包括分布在研究院和分公司机房的网络通信设备。

2）安全防护资产

安全防护资产主要配置在兰曦公司中心机房，由兰曦公司信息中心管理，此外，有部分安全设备配置在各个分公司机房。

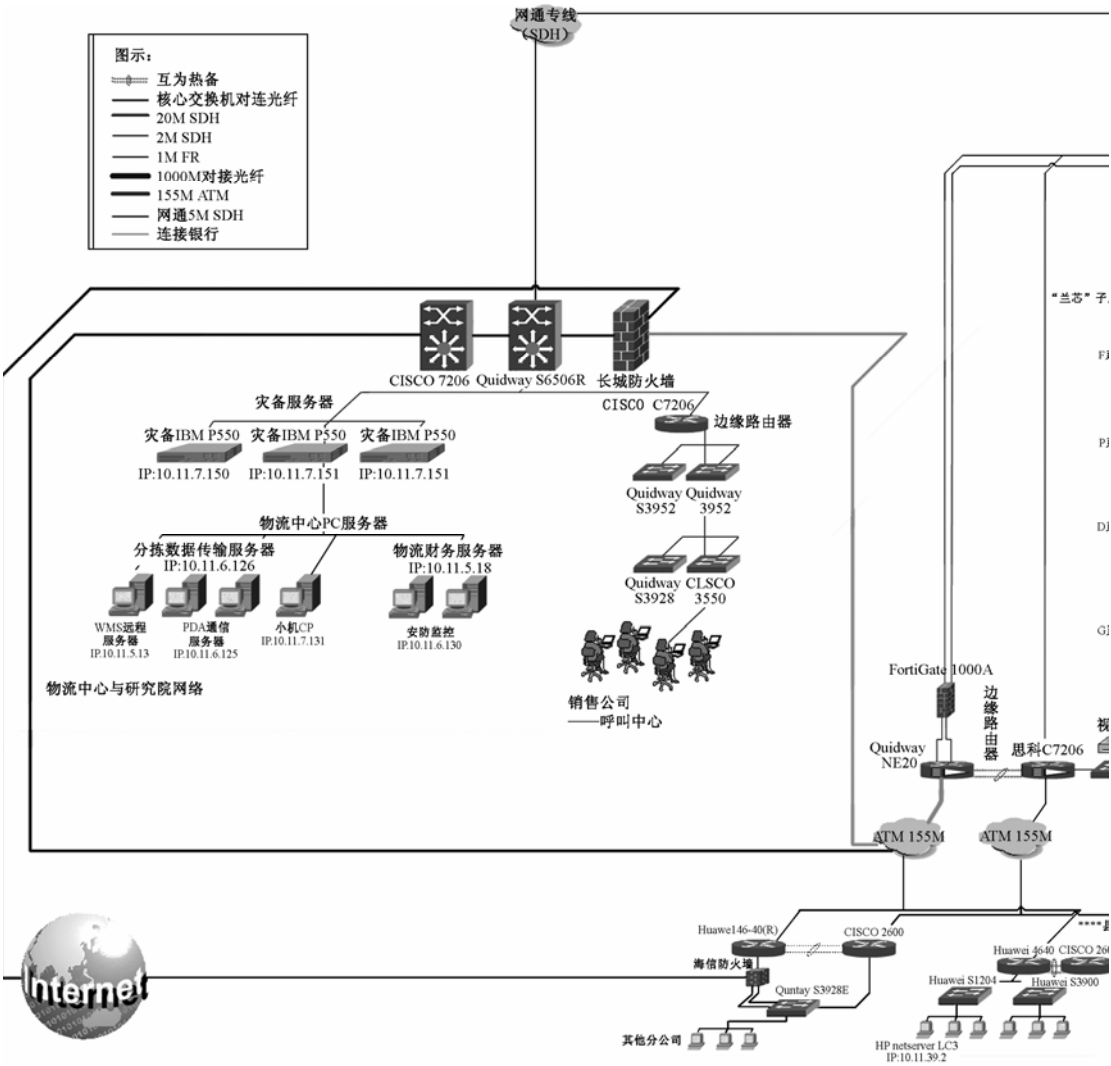
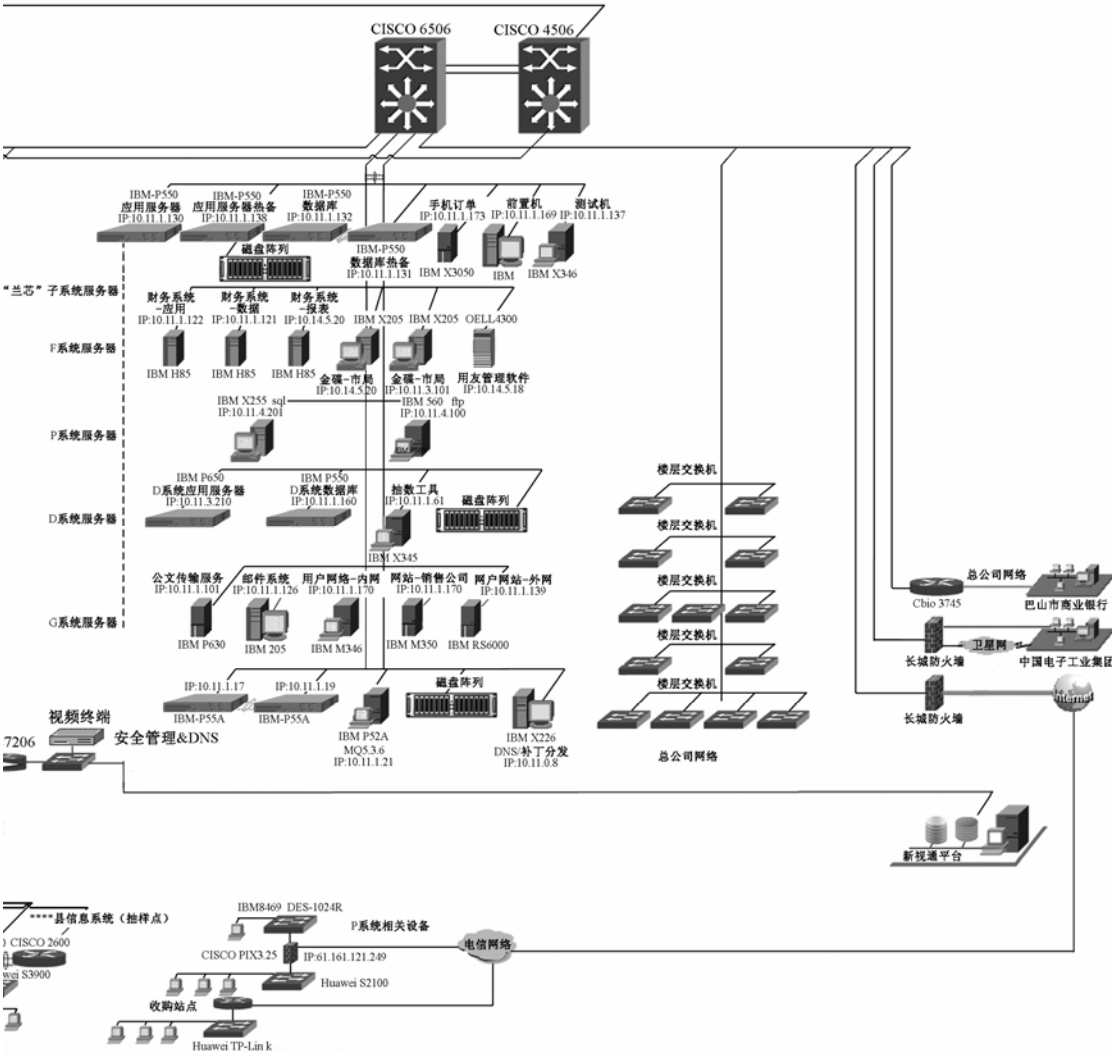

网通专线
(SDH)
图示：
互为热备
核心交换机对连光纤
20M SDH
2M SDH
1M FR
1000M对接光纤
155M ATM
网通5M SDH
连接银行
CISCO 7206
Quidway S6506R
长城防火墙
灾备服务器
灾备IBM P550
灾备IBM P550
灾备IBM P550
IP:10.11.7.150
IP:10.11.7.151
IP:10.11.7.151
物流中心PC服务器
分拣数据传输服务器
IP:10.11.6.126
物流财务服务器
IP:10.11.5.18
WMS远程服务器
IP:10.11.5.13
PDA通信服务器
IP:10.11.6.125
小机CP
IP:10.11.7.131
安防监控
IP:10.11.6.130
物流中心与研究院网络
CISCO C7206
边缘路由器
Quidway S3952
Quidway 3952
Quidway S3928
CLSCO 3550
销售公司
——呼叫中心
FortiGate 1000A
边缘路由器
Quidway NE20
思科C7206
ATM 155M
ATM 155M
Internet
Huawei46-40(R)
CISCO 2600
海信防火墙
Quntay S3928E
其他分公司
Huawei 4640
Huawei S1204
Huawei S3900
HP netserver LC3
IP:10.11.39.2

图 7.8　“数字兰曦”


CISCO 6506
CISCO 4506
IBM-P550 应用服务器 IP:10.11.1.130
IBM-P550 应用服务器热备 IP:10.11.1.138
IBM-P550 数据库 IP:10.11.1.132
手机订单 IP:10.11.1.173
前置机 IP:10.11.1.169
测试机 IP:10.11.1.137
磁盘阵列
IBM-P550 数据库热备 IP:10.11.1.131
IBM X3050
IBM
IBM X346
"兰芯"子系统服务器
财务系统-应用 IP:10.11.1.122
财务系统-数据 IP:10.11.1.121
财务系统-报表 IP:10.14.5.20
IBM X205
IBM X205
OELL4300
F系统服务器
IBM H85
IBM H85
IBM H85
金碟-市局 IP:10.14.5.20
金碟-市局 IP:10.11.3.101
用友管理软件 IP:10.14.5.18
IBM X255 sql IP:10.11.4.201
IBM 560 ftp IP:10.11.4.100
P系统服务器
IBM P650 D系统应用服务器 IP:10.11.3.210
IBM P550 D系统数据库 IP:10.11.1.160
抽数工具 IP:10.11.1.61
磁盘阵列
D系统服务器
IBM X345
公文传输服务 IP:10.11.1.101
邮件系统 IP:10.11.1.126
用户网络-内网 IP:10.11.1.170
网站-销售公司 IP:10.11.1.170
网户网站-外网 IP:10.11.1.139
IBM P630
IBM 205
IBM M346
IBM M350
IBM RS6000
G系统服务器
IP:10.11.1.17
IP:10.11.1.19
磁盘阵列
IBM-P55A
IBM-P55A
IBM P52A MQ5.3.6 IP:10.11.1.21
IBM X226 DNS/补丁分发 IP:10.11.0.8
视频终端
安全管理&DNS
楼层交换机
楼层交换机
楼层交换机
楼层交换机
楼层交换机
总公司网络
总公司网络
Cbio 3745
巴山市商业银行
卫星网
长城防火墙
中国电子工业集团
Internet
长城防火墙
新视通平台
****县信息系统（抽样点）
IBM8469 DES-1024R
P系统相关设备
CISCO 2600
CISCO PIX3.25
IP:61.161.121.249
电信网络
Huawei S2100
收购站点
Huawei TP-Lin k

网络拓扑简图


在进行网络设备和安全防护设备分类识别的时候，测评工程师可以根据与被测评单位达成的相关协议，尽可能多地了解设备型号、版本型号等信息。然而在测评过程中，也不排除被测评单位由于管理不善或集成厂商未能及时提供相关设备信息的情况。如果出现这种情况，建议测评工程师利用数码相机等对相关设备型号进行拍摄，并在各设备供应商的网站上详细了解这些设备的性能、功能。例如，在上面的例子中，有部分安全防护设备的操作系统版本型号在现场检查中就未能获得相关信息。这就需要记录下产品型号数据，然后通过供应商网站等渠道进行了解和核对。这样做的目的也是为了更详细地评估组织的信息系统建设是否真正贯彻了该组织事先制定的信息化发展目标、组织的业务战略等。在本案例中，核心交换机、路由器等设备的选型，均是为了实现兰曦公司业务战略而映射出来的资产。

3．专属信息及信息载体资产——“兰芯”子系统

兰曦公司“兰芯”子系统是从 2004 年至 2006 年由国内大型应用软件企业“快帆”公司承建开发的，整个系统的开发遵循中国电子工业集团“统一平台、统一数据库、统一网络”的规范。”兰芯”子系统主要包括营销管理、现代物流、客户关系管理、供应链管理、供应商管理、人力资源、生产管理等八个方面的应用。

作为兰曦公司最主要的生产经营系统，“兰芯”子系统使用范围覆盖了 12 家子公司、1 家研究院和全国 145 个销售网点，所有的业务应用及业务数据都集中在公司信息中心的服务器群上，呈现出明显的应用大集成、数据大集中特点。通过”兰芯”子系统的应用，实现了为全国上百家用户提供从订货到送货全流程的优质服务；实现了客户与巴山市内工、农、建、信用合作社、邮政 5 家银行中任意一家银行进行货款交易的实时扣划，加快了货款回笼，方便了客户货款支付；产品营销数据实时汇集在行业各级管理部门，实现了各级领导干部和管理人员随时了解、分析行业经济运行情况，提高了经营决策和运行调控的效率。通过对行业供应链的一体化管理，实现以市场为导向优化资源配置、提高效率、降低成本、提升效益的目的。

上面这一段分析实际上也是将兰曦公司的业务战略与“数字兰曦”进行关联，从而分析出“兰芯”子系统是实现企业业务战略的核心信息资产之一。

1）“兰芯”子系统边界识别

由于”兰芯”子系统覆盖范围广，应用面宽，并且其功能还在不断地完善，因此该系统与其他内部、外部（主要是银行）系统存在较多的信息交互，并且支撑整个”兰芯”子系统的硬件设备数量众多，地理位置上分布也比较广。由于业务及数据的集中，系统的核心设备集中分布在公司信息中心机房，但系统的下沿触角则延伸至各分公司、研究院及面向全国销售网点的最终端销售人员。系统的物理边界及逻辑边界较为复杂，要保障整个系统的可靠运行，就需要从系统信息流的产生源头、传输途径、处理及存储各个方面进行保障，如图 7.9 所示。

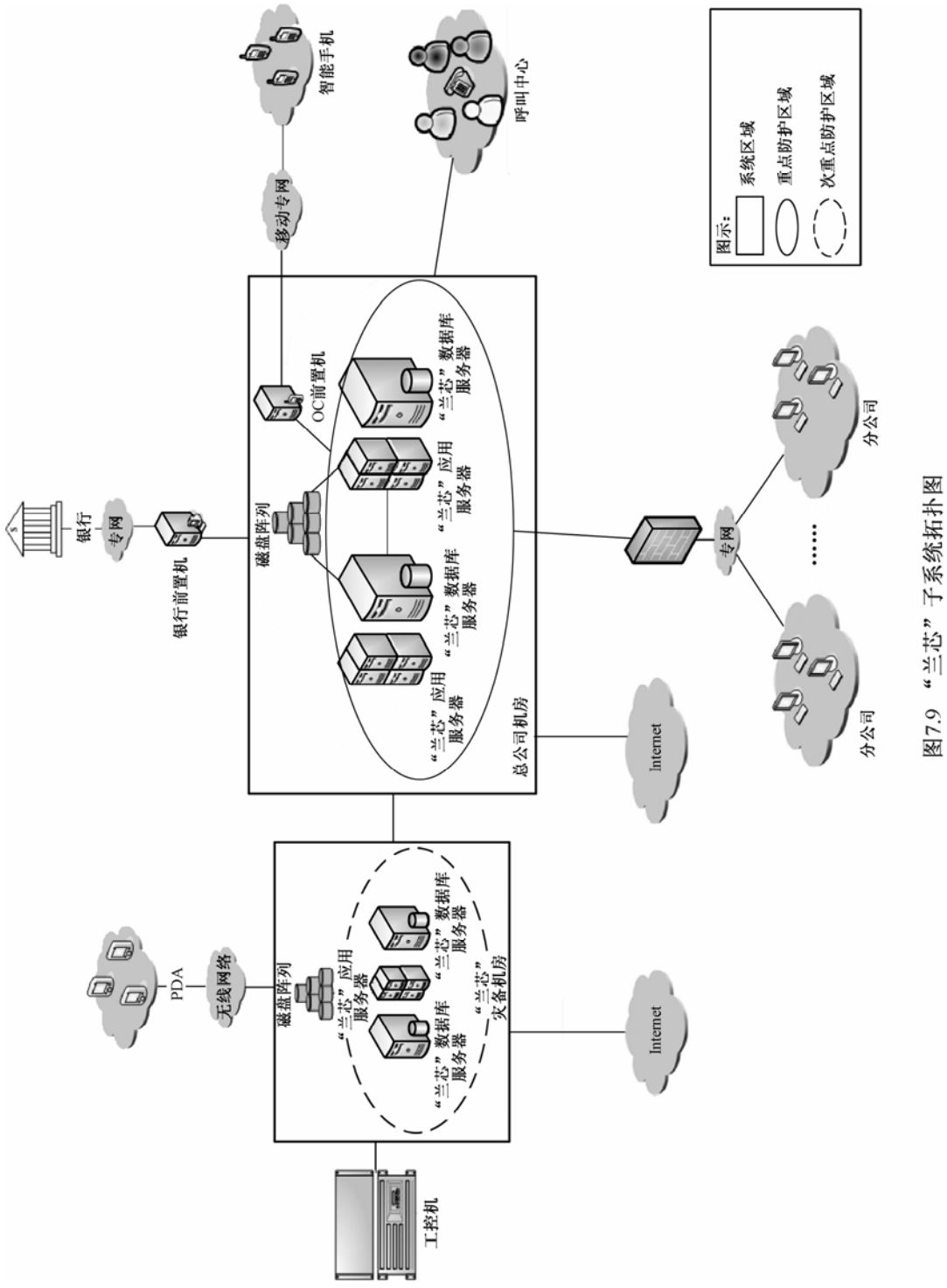


图7.9　“兰芯”子系统拓扑图

2）”兰芯”子系统业务流程描述

业务流程描述是将组织的业务战略与信息资产进行关联的重要组成部分。评估人员应当与被评估单位信息中心和业务应用部门的负责人进行充分的交流，弄清楚信息系统在该组织业务应用中的“信息流”流动环节。

“兰芯”子系统业务流程根据“四流”——商流、资金流、物流和信息流来进行描述。

商流：进货信息通过入库时与录入的进货合同数据进行对比产生的数据得出库存数据；客户管理子系统将客户订单信息转化成电子结算和配送信息分别进行电子结算和配送。商流在其整个业务流程中起着承上启下的作用，故定义 3 个风险控制点。

- 数据元的采集，客户订单直接决定电子结算和物流配送；
- 数据传输，数据的实时传输使整个业务正常的开展；
- 数据管理和存储，数据的管理和安全存储是”兰芯”子系统正常运行的前提。

上面这一段分析实际上凝练出了“兰芯”子系统需要重点识别的专用信息和信息载体资产。“兰芯”系统功能结构图如图 7.10 所示。

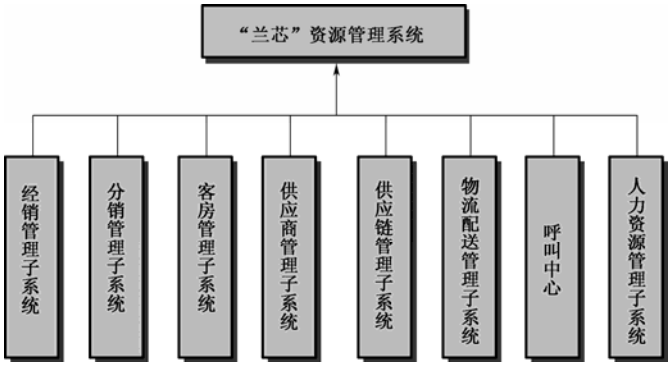


图 7.10　“兰芯”系统功能结构图

物流：收到商流生成的订单信息后开始备货，经分拣后出货（具体作业流程如图 7.11 所示）。

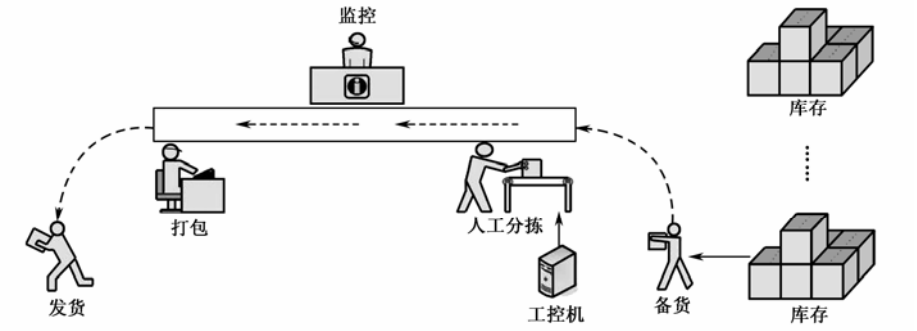


图 7.11　作业流程示意图

资金流：通过商流产生的电子结算信息与银行进行第一次电子结算，结算成功，则资金划到对应的销售分公司；结算失败，则将信息反馈给商流进行第二次电子结算。

信息流作为顶层的业务流，囊括了其他“三流”。

根据上面的信息流分析，获得了“数字兰曦”专用信息及信息载体资产分类表（由于篇幅的原因，本章仅罗列出部分资产）。

3）“兰芯”子系统专属信息载体资产

在表 7.14 中，增加了“主要用途”这一栏。这样做的目的是将各种设备资产与组织的业务相关联。资产识别的关键是将资产与组织的业务战略联系起来，这是风险评估工作中最基本、也是最关键的一步。因此，在本案例中，由于“兰芯”子系统是整个兰曦公司的核心业务子系统，所以对兰芯子系统的资产及它们的主要用途进行关联描述。

表 7.14　“兰芯”子系统信息载体资产

序号	名　　称	型　　号	数量	主 要 配 置	主 要 用 途	资产编号
1	IBM 服务器	IBM P550	2 台	CPU：4×1.5GHz 内存：8GB 硬盘：2×70GB 光纤网卡：2 个	公司“兰芯”子系统应用服务器及热备应用服务器	D_A01
2	IBM 服务器	IBM P550	2 台	CPU：4×1.5GHz 内存：16GB 硬盘：2×70GB 光纤网卡：2 个	公司“兰芯”子系统应用服务器及热备应用服务器	D_A02
3	IBM 前置机	IBM	1 台	CPU：奔 3700 内存：1GB 磁盘：50GB	公司“兰芯”子系统前置机与各大银行通信进行实时电子结算	D_A03
4	IBM 测试机	IBM X346	1 台	CPU：intel xeon3.0GHz 内存：4GB 硬盘：280GB	公司“兰芯”子系统测试机	D_A04
5	磁盘阵列		2 台	fast t600 阵列，300GB×14，raid 10	“数字兰曦”数据备份系统	D_A05
6	光交换机	IBM 3534 F08	1 台		公司“兰芯”子系统光交换机	D_A06
7	光交换机	silkworm 200E	2 台		公司“兰芯”子系统备份中心	D_A07
8	IBM 服务器	IBM P550	1 台	CPU：4×1.5GHz 内存：8GB 硬盘：2×70GB 光纤网卡：2 个	公司“兰芯”子系统备份中心应用服务器	D_A08
9	IBM 服务器	IBM P550	2 台	CPU：4×1.5GHz 内存：8GB 硬盘：2×70GB 光纤网卡：2 个	公司“兰芯”子系统备份中心数据库服务器	D_A09
10	无线路由器	CISCO aironet 1200	1 台		公司“兰芯”子系统	D_A10
	……					

4）“兰芯”子系统软件资产

由于篇幅原因，我们只是有代表性地选择了部分软件资产，主要包括各种操作系统、数据库、中间件等。在表 7.15 中，除了对软件资产的主要用途进行描述外，又增加了“使用范围”这一栏，这是因为软件资产的使用范围比硬件设备更广，如交换机一般只会放置在中心机房，而操作系统等软件则会一直延伸到各个终端。

表 7.15　“兰芯”子系统软件资产

序号	名　称	版　本	数量	开发商	主要用途	使用范围	资产编号
1	Aix 操作系统	Aix 5.3	7 套	惠普	“兰芯”子系统服务器操作系统	信息中心	D_SF01
2	Windows 操作系统	Windows 2003	1 套	微软	“兰芯”子系统服务器操作系统	信息中心	D_SF02
3	Windows 操作系统	Windows 2000	1 套	微软	“兰芯”子系统服务器操作系统	信息中心	D_SF03
4	DB2		4 套		“兰芯”子系统数据库服务器	信息中心	D_SF04
5	Websphere		3 套		“兰芯”子系统中间件	信息中心	D_SF05
6	“兰芯营销”系统		3 套		“兰芯”子系统应用软件	信息中心	D_SF06
7	用友华表 cell 组件		1 套		“兰芯”子系统组件	信息中心	D_SF07
8	SQL Server		1 套		“兰芯”子系统数据库	信息中心	D_SF08
9	RemoteServer 服务端		1 套		“兰芯”子系统组件	研究院	D_SF09
10	PDA 客户端		1 套		“兰芯”子系统应用软件	研究院	D_SF10
	……						

5）“兰芯”子系统数据资产

由于篇幅原因，我们只是有代表性地选择了部分数据资产，主要包括专用 IP 地址、组织核心业务电子文档等。需要指出的是，这部分资产往往是一个组织的核心资产。例如，我们在表 7.16 中可以看到“兰芯系统运营销售业务统计报告”这个电子文档。它所记载的是“兰芯”子系统覆盖全国的销售网络的营销数据，是一个企业的核心敏感数据之一。因此，在该份电子文档的“共享范围”一栏中，根据现场调研了解到的情况，对其注明“由公司决策层授权，公司销售部门使用”的字样。

表 7.16　“兰芯”子系统数据资产

序号	名　　称	类　　型	数量	共 享 范 围	资产编号
1	10.11.1.130	IP 地址	1 个	“兰芯”子系统专用服务器专用地址，公司总部使用	D_D01
2	10.11.1.138	IP 地址	1 个	“兰芯”子系统专用服务器专用地址，信息中心使用	D_D02
3	“兰芯”子系统操作手册	电子文档	1 个	公司各业务部门使用	D_D12
4	“兰芯”子系统维护手册	电子文档	1 个	信息中心专用	D_D15
5	“兰芯”子系统运行规范	电子文档	1 个	信息中心专用	D_D16
6	“兰芯”子系统运行管理办法	电子文档	1 个	信息中心专用	D_D17
7	“兰芯”子系统项目管理规范	电子文档	1 个	公司销售部门使用	D_D18
8	“兰芯”子系统运营销售业务统计报告	电子文档	1 个	公司决策层授权，公司销售部门使用	D_D19
9	“兰芯”子系统总体规划	电子文档	1 个	信息中心专用	D_D20
10	“兰芯”子系统基础数据编码规则	电子文档	1 个	研究院、信息中心	D_D21
11	“兰芯”子系统需求调研方案	电子文档	1 个	信息中心专用	D_D22
12	“兰芯”子系统项目需求说明书	电子文档	1 个	信息中心专用	D_D23
13	“兰芯”子系统项目设计说明书	电子文档	1 个	信息中心专用	D_D24
14	“兰芯”子系统集群结构方案	电子文档	1 个	辅助决策系统专用	D_D25
15	“兰芯”子系统业务数据库和历史数据库汇总技术方案	电子文档	1 个	辅助决策系统专用	D_D26
	……				

在这里罗列了许多软件和数据资产，可能对于初学者而言会觉得不知所措。事实上，这样做的主要目的就是让读者了解到对于一个组织而言，其专用信息资产是非常丰富的，它是组织的业务战略在信息系统中最细致的体现。例如，兰曦公司的决策部门通过对“运营销售业务统计报告”等资料的分析，就能实时掌握公司的行业竞争力在全国乃至全球范围内是处于什么位置；对”兰芯”子系统设计手册、所依赖的操作系统和中间件等的研究，就能够发现该系统可能面临什么样的威胁或脆弱性等。这些都是进行风险评估和安全保护的核心资产。

7.3.3　资产赋值

作为本章正文的结尾，将对“数字兰曦”的信息环境资产、公用信息载体资产和专用信息及信息载体资产进行赋值。在实际工作中，资产赋值往往是“经验赋值”，即根据测评人员的工程经验和被测单位的业务情况进行赋值。要特别注意在赋值过程中应该与被测评单位的各级人员，特别是信息中心的管理人员和技术人员进行充分的沟通和交流。要发挥他们熟悉本单位业务情况的作用及信息安全风险评估专业人员在安全技术方面的优势，共同决定各种资产的赋值。

1．信息环境资产赋值

1）人员资产赋值

如果严格地按照信息安全的“保密性、完整性和可用性”来对人员资产进行赋值，就显得非常教条了（想象一下人员完整性应该如何赋值？）。因此根据其工作岗位描述进行赋值，如根据“信息化是一把手工程”这一实际工作经验，应当将兰曦公司信息化领导小组成员的资产价值赋值为最高的“5”，然后依此类推，如表 7.17 所示。

表 7.17　人员资产赋值

序号	人 员 资 产	关 联 资 产	资 产 价 值
1	公司信息化领导小组成员	“数字兰曦”	5
2	公司信息中心信息化人员	“数字兰曦”	4
3	分公司或研究院信息化人员	下属单位信息系统	3
	……		

2）人员重要性等级赋值

人员重要性等级赋值如表 7.18 所示。

表 7.18　人员重要性等级赋值

序号	人 员 资 产	资 产 价 值	资 产 等 级	资产等级值
1	公司信息化领导小组成员	5	很高	5
2	公司信息中心信息化人员	4	高	4
3	分公司或研究院信息化人员	4	高	3
	……			

接下来所进行的赋值，则可以按照信息安全的三个属性及它们在实现组织业务战略中的作用进行赋值。要注意在赋值过程中评估人员和被评估单位（特别是信息中心）有关人员进行磋商，共同决定每一项资产的价值和重要性。在下面的赋值中，均是按照“保密性、完整性、可用性”三个属性中的最高等级来取值的（请参见 7.2 节有关资产赋值的内容）。

3）管理制度资产赋值

在表 7.19 中，资产价值和资产等级为 4 的管理制度资产是测评人员重点关注的管理资产。这些制度是否得以真正贯彻落实，是被测单位信息安全管理是否到位的体现。顺便指出，在进行风险评估过程中，测评人员还应当核对各种管理制度的支撑材料，如各种管理制度的版本更新记录、审核记录、培训记录等，这些记录实际上才能真正反映出一个组织的信息安全管理制度是否得以落实（参见第 13 章“信息安全管理体系”）。

4）管理制度重要性赋值

管理制度重要性赋值如表 7.20 所示。

表 7.19　管理制度资产赋值

序　号	人 员 资 产	关 联 资 产	资 产 价 值
1	《中心机房管理办法》	公司信息中心	4
2	《“数字兰曦”视频会议系统运行管理办法》	“数字兰曦”	3
3	《“数字兰曦”网络建设及管理规范》	“数字兰曦”	4
4	《“数字兰曦”网络安全管理办法》	“数字兰曦”	4
5	《兰曦公司关于加强行业互联网管理工作的通知》	“数字兰曦”	4
6	《中国电子工业集团关于加强计算机信息系统安全管理的通知》	“数字兰曦”	4
	……		

表 7.20　管理制度重要性赋值

序号	人 员 资 产	资 产 价 值	资 产 等 级	资产等级值
1	《中心机房管理办法》	4	高	4
2	《“数字兰曦”视频会议系统运行管理办法》	3	中	3
3	《“数字兰曦”网络建设及管理规范》	4	高	4
4	《“数字兰曦”网络安全管理办法》	4	高	4
5	《兰曦公司关于加强行业互联网管理工作的通知》	4	高	4
6	《中国电子工业集团关于加强计算机信息系统安全管理的通知》	4	高	4
	……			

5）系统机房资产赋值

毫无疑问，整个“数字兰曦”系统机房资产价值最高的是公司的中心机房。其次是研究院所属的专用机房，因为研究院承担的工作是从事兰曦公司核心产品的研发，其各种技术资料均存储在该机房的数据库服务器等设备之中，如表 7.21 所示。

表 7.21　系统机房资产赋值

序号	人 员 资 产	资 产 编 号	所 属 部 门	资 产 价 值
1	公司中心机房	JF01	信息中心	5
2	研究院中心机房	JF02	研究院	4
3	分公司中心机房	JF03	各个分公司	3
	……			

6）系统机房重要性赋值

系统机房重要性赋值如表 7.22 所示。

表 7.22　系统机房重要性赋值

序号	人 员 资 产	资 产 价 值	资 产 等 级	资产等级值
1	公司中心机房	5	很高	5
2	研究院中心机房	4	高	5
3	分公司中心机房	4	中	3
	……			

至此，我们对“数字兰曦”信息环境资产进行了赋值。接下来进入“数字兰曦”公用信息载体的资产赋值环节。

2．公用信息载体资产赋值

在 7.3.2 节中分析了公用信息载体资产，将它分为网络设备和安全防护设备两大类，下面就分别对 7.3.2 节中的表 7.12 和 7.13 进行赋值。

1）网络设备资产赋值

按照在表 7.12“通信载体资产”中的描述，可以得知哪些网络设备的资产价值较高，如“核心交换机 CISCO 6506”、“QuidWay S6506R”等。此外，在表 7.23 中，CISCO 3825 路由器是兰曦公司连接中国电子工业集团（纵向连接）和巴山市电子政务内网（横向连接）的设备，所以根据与兰曦公司信息中心技术人员的讨论，该项资产的赋值也较高，如表 7.23 所示。

表 7.23　网络设备资产赋值

序号	名　　称	型　　号	所 属 系 统	资 产 价 值
1	核心交换机	CISCO 6506	“数字兰曦”	5
2	核心交换机	CISCO 4506	“数字兰曦”	5
3	楼层交换机 10	CISCO 3550 系列	信息中心	2
4	交换机	s5126	信息中心	3
5	交换机	QuidWay S6506R	“兰芯”子系统	5
6	交换机（研究院）	QuidWay S3952P/S3928P	研究院楼层交换	2
7	交换机（分公司）	QuidWay S3928P	分公司机房	2
8	核心路由器	QuidWay NE20 （OSPF 路由协议）	连接分公司	3
9	核心备份路由器	CISCO 7206 （OSPF 路由协议）	连接分公司	3
10	路由器（连接银行）	CISCO 3745 （静态路由）	“兰芯”子系统	4
11	路由器（连接中国电子工业集团及巴山市电子政务内网）	CISCO 3825 （BGP 路由协议）	信息中心	4
12	路由器	QuidWay AR4640（OSPF 路由协议）	分中心机房	2
				

细心的读者可能还会发现，表 7.23 中有 1 台连接到兰曦公司的上级单位——中国电子工业集团和巴山市电子政务内网的交换机运行的是 CISCO 3825（BGP 路由协议）。下面这个典故也许对从事风险评估的人员有些启迪。

由此可见，在进行资产识别的工作中，应当尽量了解各种资产的详细信息，同时发挥测评人员在信息安全专业知识方面的长处（由于工作分工不同，被测单位信息中心的人员一般不会对设备面临的安全隐患有更加深入的跟踪分析），对所了解到的各种技术参数进行分析。



近日两名美国黑客演示了一种新技术，可以截获 Internet 上的数据包，这种截获方式以前曾被认为不可能实现。该技术利用 Internet 路由协议 BGP（Border Gateway Protocol），让入侵者监视世界上任何地方的 Internet 数据流，甚至可以对数据包进行篡改，该攻击还利用 BGP 协议欺骗路由器将数据转发到窃听网络上。事实上，有关研究人员对 BGP 协议的漏洞已经研究了二十多年。

该演示只是为了显示 Internet 核心协议在安全方面的不足，Internet 核心协议多数开发于 20 世纪 70 年代，基于当时初生的网络，人们假设网络上的节点都是可信的。这些假设正被一一击破。

2）网络设备资产重要性赋值

网络设备资产重要性赋值如表 7.24 所示，其中 CISCO 3825 设备赋值较高。

表 7.24　网络设备资产重要性赋值

序号	名　　称	资 产 价 值	资 产 等 级	资产等级值
1	核心交换机	5	很高	5
2	核心交换机	5	很高	5
3	楼层交换机	2	低	2
4	交换机	3	中等	3
5	交换机	5	很高	5
6	交换机（研究院）	2	低	2
7	交换机（分公司）	2	低	2
8	核心路由器	3	中等	3
9	核心备份路由器	3	中等	3
10	路由器（连接银行）	4	高	4
11	路由器（连接中国电子工业集团及巴山市电子政务内网）	4	高	4
12	分公司路由器	2	低	2
	……			

3）安全防护资产赋值

在对安全防护资产进行赋值时，读者可以看到处于网络边界防护位置的设备赋值较高，如互联网防火墙 4000V2、广域网防火墙 FortiGate 1000A 等。此外，由于漏洞扫描设备是发现系统漏洞的最主要工具，它的使用频率较高，需要进行严格管理（包括漏洞库的升级等），因此赋值为“5”，如表 7.25 所示。

表 7.25　安全防护设备资产赋值

序号	名　称	型　号	资产编号	所属系统	资产价值
1	互联网防火墙	4000V2	X_FH01	信息中心	4
2	广域网防火墙	FortiGate 1000A	X_FH02	连接分公司	4
3	分公司防火墙	POWER-V 404	X_FH03	连接分公司	3
4	分公司防火墙	NETPOWER	X_FH04	连接分公司	2
5	“冰之眼”入侵检测	1600D	X_FH05	信息中心	3
6	“天眼”入侵检测	NPIDS-100	X_FH06	信息中心	2
7	主机入侵检测	QuidWay S3928P	X_FH07	信息中心	4
8	“极光”漏洞扫描	“极光 V4”	X_FH09	信息中心	5
	……				

4）安全防护资产重要性赋值

安全防护设备重要性赋值如表 7.26 所示。

表 7.26　安全防护设备重要性赋值

序号	名　称	型　号	资产价值	资产等级	资产等级值
1	互联网防火墙	4000V2	4	高	4
2	广域网防火墙	FortiGate 1000A	4	高	4
3	分公司防火墙	POWER-V 404	3	中等	3
4	分公司防火墙	NETPOWER	2	较低	2
5	“冰之眼”入侵检测	1600D	3	中等	3
6	“天眼”入侵检测	NPIDS-100	2	较低	2
7	主机入侵检测	QuidWay S3928P	4	高	4
8	“极光”漏洞扫描	“极光 V4”	5	很高	5
	……				

至此，我们完成了对“数字兰曦”公用信息载体资产的赋值。下面进入专用信息资产赋值的环节。

3．专用信息及信息载体资产赋值——“兰芯”子系统资产赋值

1）“兰芯”子系统硬件资产赋值

“兰芯”子系统是整个“数字兰曦”的核心子系统。对“兰芯”子系统硬件资产的赋值是按照信息安全的 3 个属性来确定的，如表 7.27 所示。例如，资产编号为 D_A01 的 IBM P550 设备，主要为“数字兰曦”提供基础的网络交换功能，因此系统的可用性要求最高，而资产编号为 D_A03 的 IMB 前置机，由于它在“数字兰曦”系统中扮演的是与各大银行进行数据交换的角色，因此无论是保密性、完整性还是可用性要求都很高。总之，“兰芯”子系统的硬件资产赋值是根据对“兰芯”子系统进行资产识别的时候（见表 7.14、表 7.15 和表 7.16 等）而确定的。

表 7.27　“兰芯”子系统硬件资产赋值

序号	名　　称	型　　号	资产编号	保密性	完整性	可用性	资产价值
1	IBM 服务器	IBM P550	D_A01	4	4	5	5
2	IBM 服务器	IBM P550	D_A02	5	3	4	5
3	IBM 前置机	IBM	D_A03	5	5	5	5
4	IBM 测试机	IBM X346	D_A04	2	2	3	3
5	磁盘阵列	—	D_A05	4	5	5	5
6	光交换机	IBM 3534 F08	D_A06	2	3	5	5
7	光交换机	silkworm 200E	D_A07	2	3	5	5
8	IBM 服务器	IBM P550	D_A08	4	5	5	5
9	IBM 服务器	IBM P550	D_A09	5	5	5	5
10	IBM 服务器	IBM　xServer226	D_A10	4	4	4	4
11	无线路由器	cisco aironet 1200	D_A11	2	3	3	3
							

2）“兰芯”子系统硬件资产重要性赋值

“兰芯”子系统硬件资产重要性赋值如表 7.28 所示。

表 7.28　“兰芯”子系统硬件资产重要性赋值

序号	名　　称	资 产 编 号	资 产 价 值	资 产 等 级	资产等级值
1	IBM 服务器	D_A01	5	很高	5
2	IBM 服务器	D_A02	5	很高	5
3	IBM 前置机	D_A03	5	很高	5
4	IBM 测试机	D_A04	3	中等	3
5	磁盘阵列	D_A05	5	很高	5
6	光交换机	D_A06	5	很高	5
7	光交换机	D_A07	5	很高	5
8	IBM 服务器	D_A08	5	很高	5
9	IBM 服务器	D_A09	5	很高	5
10	IBM 服务器	D_A10	4	高	4
11	无线路由器	D_A11	3	中等	3
					

3）“兰芯”子系统软件资产赋值

“兰芯”子系统软件资产中，Aix 操作系统配置在 IBM 服务器上，所以相应的保密性、完整性和可用性赋值与硬件赋值相一致。DB2 是“兰芯”子系统重要的数据库，对其保密性、完整性和可用性的要求均很高，所以资产价值也最高。而 Websphere 中间件是“兰芯”子系统业务应用软件的核心，所以在完整性、可用性等方面要求也达到了 5 级，如表 7.29 所示。

表 7.29　“兰芯”子系统软件资产赋值

序号	名　称	资产编号	保密性	完整性	可用性	资产价值
1	Aix 操作系统	D_SF01	4	4	5	5
2	Windows 操作系统	D_SF02	5	3	4	5
3	Windows 操作系统	D_SF03	2	2	3	3
4	DB2	D_SF04	5	5	5	5
5	Websphere	D_SF05	4	5	5	5
6	“兰芯”子系统	D_SF06	5	5	5	5
7	用友华表 cell 组件	D_SF07	3	3	3	3
8	SQL Server	D_SF08	2	2	3	3
9	RemoteServer 服务端	D_SF09	3	4	4	4
10	PDA 客户端	D_SF10	3	3	3	3
						

4）“兰芯”子系统软件资产重要性赋值

“兰芯”子系统软件资产重要性赋值如表 7.30 所示。

表 7.30　“兰芯”子系统软件资产重要性赋值

序号	名　称	资产编号	资产价值	资产等级	资产等级值
1	Aix 操作系统	D_SF01	5	很高	5
2	Windows 操作系统	D_SF02	5	很高	5
3	Windows 操作系统	D_SF03	3	中等	3
4	DB2	D_SF04	5	很高	5
5	Websphere	D_SF05	5	很高	5
6	“兰芯”子系统	D_SF06	5	很高	5
7	用友华表 cell 组件	D_SF07	3	中等	3
8	SQL Server	D_SF08	3	中等	3
9	RemoteServer 服务端	D_SF09	4	高	4
10	PDA 客户端	D_SF10	3	中等	3
					

5）“兰芯”子系统数据资产赋值——文档部分

根据上面对“兰芯”子系统数据资产的识别（见表 7.16），对文档资产的赋值如表 7.31 所示，其中”兰芯”子系统运行业务统计报告的保密性要求最高、完整性和可用性也有较高要求。

表 7.31　“兰芯”子系统文档资产赋值

序号	名　称	保密性	完整性	可用性	资产价值
1	“兰芯”子系统操作手册	3	3	3	3
2	“兰芯”子系统维护手册	3	3	3	3

续表

序号	名　　称	保 密 性	完 整 性	可 用 性	资 产 价 值
3	“兰芯”子系统运行规范	3	3	3	3
4	“兰芯”子系统运行管理办法	3	3	3	3
5	“兰芯”子系统项目管理规范	2	2	2	2
6	“兰芯”子系统运行业务统计报告	5	4	4	5
7	“兰芯”子系统总体规划	2	2	2	2
8	“兰芯”子系统基础数据编码规则	2	2	2	2
9	“兰芯”子系统需求调研方案	2	2	2	2
10	“兰芯”子系统项目需求说明书	2	2	2	2
11	“兰芯”子系统项目设计说明书	2	2	2	2
12	“兰芯”子系统集群结构方案	2	2	3	3
13	“兰芯”子系统业务数据库和历史数据库汇总技术方案	4	4	3	4
	……				

6）“兰芯”子系统数据资产重要性赋值——文档部分

“兰芯”子系统文档资产重要性赋值如表 7.32 所示。

表 7.32　“兰芯”子系统文档资产重要性赋值

序号	名　　称	类　　型	资产价值	资产等级	资产等级值
1	“兰芯”子系统操作手册	电子文档	3	中等	3
2	“兰芯”子系统维护手册	电子文档	3	中等	3
3	“兰芯”子系统运行规范	电子文档	3	中等	3
4	“兰芯”子系统运行管理办法	电子文档	3	中等	3
5	“兰芯”子系统项目管理规范	电子文档	2	低	2
6	“兰芯”子系统运销业务统计报告	电子文档	5	很高	5
7	“兰芯”子系统总体规划	电子文档	2	低	2
8	“兰芯”子系统基础数据编码规则	电子文档	2	低	2
9	“兰芯”子系统需求调研方案	电子文档	2	低	2
10	“兰芯”子系统项目需求说明书	电子文档	2	低	2
11	“兰芯”子系统项目设计说明书	电子文档	2	中等	2
12	“兰芯”子系统集群结构方案	电子文档	3	中等	3
13	“兰芯”子系统业务数据库和历史数据库汇总技术方案	电子文档	4	高	4
	……				

7）“兰芯”子系统数据资产赋值——IP地址部分

“兰芯”子系统数据资产中专门将 IP 地址单列出来，因为这部分 IP 地址对应与“兰芯”子系统的核心设备。要注意没有按照信息安全的保密性、完整性和可用性来分别对 IP 地址进行赋值，而是根据经验进行综合赋值，如表 7.33 所示。

表 7.33　“兰芯”子系统 IP 地址资产赋值

序号	名　称	类　型	资产编号	关联资产	资产价值
1	10.11.1.130	IP 地址	D_D01	D_A01	4
2	10.11.1.138	IP 地址	D_D02	D_A01	4
	……				

8）“兰芯”子系统数据资产重要性赋值——IP地址部分

“兰芯”子系统 IP 地址资产重要性赋值如表 7.34 所示。

表 7.34　“兰芯”子系统 IP 地址资产重要性赋值

序号	名　称	资产价值	资产等级	资产等级值
1	10.11.1.130	4	高	4
2	10.11.1.138	4	高	4
	……			

7.3.4　资产识别输出报告

在完成了对“数字兰曦”各项资产的识别和赋值之后，最后要完成一个文档性的工作，即应该输出一份技术报告——《资产识别报告》。报告的主体包括被评估单位系统描述、资产分类、资产赋值等。以本节案例为例，该报告的内容排序如下：

“深海”信息安全测评中心

“数字兰曦”资产识别报告

摘要
目录
图标目录
报告审批（授权签字）及日期
1　撰写依据
2　术语解释
3　资产分类原则和方法
4　“数字兰曦”系统描述
5　“数字兰曦”资产识别
5.1　“兰芯”子系统资产识别
5.2　“兰剑”子系统资产识别
5.3　……
6　附录

错误！

7.4　本章小结

- 信息安全风险的概念
- 风险与安全的关系
- 风险评估的本质思想
- 威胁、脆弱性和风险的关系
- 资产和资产识别的关系
- 风险评估与等级保护的关系
- 风险评估的难点
- 资产分类的两种主要方法
- 礼花模型
- 资产识别的主要环节
- 资产赋值包括的内容
- 资产识别完成后应输出的报告

尾声：我们究竟拥有什么？

如果“我们”是指人类，那么我们拥有一个地球，以及月球；还拥有一个太阳，以及整个太阳系。当然还可以说我们拥有整个银河系——亘古至今，有谁曾与我们争过呢。同理还可以说，我们拥有宇宙间所有的星系——亘古至今，又有谁曾与我们争过呢。那么，也就可以说，我们拥有整个宇宙——即便有地外文明的存在，最多也只是跟我们捉迷藏似的不时“暗斗”一下，似乎还不曾“斗胆”与我们“明争”过……是的，虽然我们“拥有”整个宇宙，可是我们能够直接“享用”的，不过就是小小太阳，区区地球而已。

如果“我们”是指一个民族，那么我们拥有啼鸣雄鸡状的广袤国土，拥有 5000 年绵延不断的灿烂文明；还拥有这被称为和平崛起的新时代，还拥有刚刚过去的将被深深铭刻在史上的梦幻般的 2008 年奥运会……

如果“我们”是指一个个的人、一个集体、一个组织机构……，那么我们会拥有所谓的“资产”。但是，重要的却不在于此。重要的是，“资产”这个东西，随着历史不断向前推进，它的内涵正在发生着深刻的变化——从有形到无形，从物质到信息，从躯壳到智慧……

我们——你、我、他——拥有新鲜的空气、温暖的阳光，还有满足生命渴望的水；我们还（要）拥有爱、尊严及灵魂的归属；（要）拥有生命的意义和无限的绚丽……总之，我们还（要）拥有和平的世界、安全的世界——因而才是美好的世界。

观感

（1）什么是 Abraham Maslow 层次需求理论？请上网查阅相关资料。你对这个理论和信息安全风险评估相结合有什么看法？

（2）如果您有一台自用的计算机，试根据自己的学习/工作兴趣、范围和职业发展方向等（也就是自己的业务战略）来进行自己的信息资产识别。您最重要的资产是什么？

（3）试分析您所在单位的业务战略，如数字化校园的业务战略是什么？

（4）结合上题的分析，给出您所在单位的一个资产重要性等级表，并定出该信息系统的安全等级。资产重要性等级一定与信息系统的安全等级相一致吗？

（5）请在本章案例分析的基础上给出《“兰芯”子系统资产识别报告》。

（6）在本书第 3 章《数据安全测评技术》的“观感”中，给出了“杜甫”社保信息系统的主要职能。请分析该系统的业务战略及信息安全战略。

（7）请根据“杜甫”社保信息系统的网络拓扑图并结合其业务战略，对其进行资产识别并给出《“杜甫”社保信息系统资产识别报告》。

（8）一个信息系统的资产识别过程和结果对该系统的安全等级划分起到什么作用？

第 8 章

威 胁 识 别





SARS 病毒

从原理上来讲，计算机可以模仿人类的智能，甚至比人类更好。其结果是在未来数百年中的某一天，计算机可能在智能方面取代人类。

——史蒂芬·霍金

序幕：威胁在哪里？

机遇垂青那些睁眼睡觉的人；威胁喜爱那些睁眼快睡着的人。

公元 1187 年 7 月 3 日，威风凛凛的耶路撒冷城防司令雷蒙将军率领十字军骑士们手持长矛，身裹铁甲，豪情冲天地准备与来自大马士革的穆斯林勇士们决一死战，他们渴望着与对手一刀一枪的决一雌雄。而风度翩翩的阿拉伯民族英雄萨拉丁却站在上风处命人点燃了太巴列湖边的灌木丛，把骑士们呛得半死……13 天后圣城耶路撒冷易主。

公元 2007 年 9 月 5 日，大马士革郊区导弹阵地上，最先进的俄制“道尔”防空系统雷达转动，剑指蓝天。叙利亚士兵严阵以待。以色列空军驾驶着“显形”战机却大摇大摆地穿过了叙军防区，然后彻底炸毁了叙利亚的秘密设施。事后有分析指出（CCTV“国防军事频道”——现代电子战），以色列战机使用了美国 BEA 系统公司的电子对抗吊舱，将虚假信息注入到“道尔”雷达接收天线之中，使得叙军值班人员在屏幕上没有发现任何异常现象。

在海、陆、空、天、电五维空间，威胁无孔不入……

要点：本章结束之后，读者应当了解和掌握

- 什么是威胁和威胁识别？
- 什么是重点识别和全面识别？
- 怎样进行威胁识别？植树、剪枝和统计分别起什么作用？
- 威胁识别过程要注意什么问题？
- 什么是威胁识别过程的量体裁衣？
- 威胁识别完成后应当输出哪些文档？

8.1　威胁概述

本节将介绍信息安全风险评估中的第二个环节——**威胁**和**威胁识别**的概念。自然界中有很多威胁识别起来比较容易，如台风，因为台风在气象卫星的云图上的特征很明显，破坏形式也比较单一。也有很多破坏形式很单一的威胁却难以及时识别，如地震。还有更多的威胁特征丰富多彩，需要分类识别，如金融市场上各种投机的“热钱”，虚拟空间中的各种病毒、间谍软件等。在进行信息安全风险评估的时候，来自虚拟空间的各种威胁和真实空间的各种威胁（如自然灾害）均是人们可能关注的内容。下面首先给出威胁的定义。


威胁（threat），指可能导致对系统或组织危害的事故潜在起因。

这里有几个容易混淆的概念需要澄清一下。

1．外因和外部

在第 7 章曾经讲过，威胁是安全事件发生的外因。但是要注意，这里说的外因和“外部”不完全是一个同义语。例如，一家 IT 企业的核心技术资料失窃，最后发现是因为内部骨干技术人员集体辞职准备另起炉灶造成的，这种威胁显然来自企业内部。随着网络的互联互通越来越广，业务应用越来越宽，一个组织的信息系统面临的安全威胁越来越呈现出“内外夹攻”的态势。

2．真假和虚实

这里所讨论的信息安全威胁，与更一般意义下的风险评估中的威胁侧重点有所不同。虽然现实社会中的威胁，如洪水、地震、雷电等有些是属于评估的内容（但也有些不是，如 SARS 病毒），但人们更为关注的是那些虽然发生在虚拟空间中，但却也带来真实危害的威胁。例如，由于软件故障、网络设备故障和黑客攻击行为等原因导致的航空管制系统的紊乱、供电系统中断造成的手术停顿等。当然，完全可以预计，随着人类社会对信息系统的依赖性日渐提高，一般意义下的威胁与本书所涉及的威胁会趋于一致。

知己先知彼，无论人们是否感受到它们，威胁是客观存在的。因此就需要对这些潜在的危害进行识别。


威胁识别（threat recognition），指分析事故潜在起因的过程。


威胁识别可以分为**重点识别**和**全面识别**。所谓“重点”识别，就是按照资产重要性进行排序，从而决定威胁识别的巨细程度和投入多少识别资源（评估人员、设备和时间

等)。这种方法适用于以下信息系统。

（1）网络结构重心突出，层次分明。例如，一个大型信息系统被分为了1、2、3 级三个分系统。这时威胁识别的重点毫无疑问首先应该放在最重要的3 级分系统上，然后依次类推。

（2）系统结构具有较大的同质性。例如，总行、分行，总局、分局等这种纵向管理的行业信息系统。

所谓“全面”识别，就是对每一个资产可能面临的所有威胁都要进行详细分析，而不管资产本身重要程度的高低。这种方法适用于以下情况。



MIT 校园文化诞生的黑客清誉大概是葬送在 Kevin Mitnick 手中的。这位仁兄虽然极少使用编程工具，但却绝顶聪明。20 世纪七八十年代，他在对信息系统实施攻击的时候，绝大多数情况下都是采用所谓的“社交工程”（social engineering）手段，而不是技术手段。他攻击的目的非常简单，就是为了经济利益。因此无论是电话公司的长途电话卡，还是有极大诱惑力的 IT 企业的核心源代码均是他狩猎的对象。他也因此成为 FBI 第一个“网上追逃”（most wanted）的黑客罪犯。

（1）信息系统本身处于变化和调整的阶段。例如，系统进行根本性升级换代时期。此时资产的重要性可能会进行调整，但由于新的系统还未完全建成，重要性不明，所以对老系统和即将进入的新系统都需要进行较全面的威胁识别。

（2）安全等级较高（4、5 级）的核心信息系统。此时所有资产都非常重要，需要进行安全威胁的逐一识别。例如，国家要害部门信息系统。

从可操作性的角度来讲，重点识别是风险评估工作的主要方法，符合“有所为，有所不为”的系统科学思想。此外，进行了全面识别的系统，如果变化不大，以后进行定期威胁识别的时候就可以进行抽查，从而也就转化成重点识别，这就如同软件测试中的回归测试（regression test）方法一样。

无论是重点识别还是全面识别，它们遵循的是相同的识别流程。下面进入本章的主要内容。

8.2　威胁识别的诸方面

与资产识别相类似，威胁识别分为**威胁分类**和**威胁赋值**两个环节。威胁识别的方法形象地讲就是“植树、剪枝、统计”。下面一一解释这几个词的含义。

8.2.1　威胁分类——植树和剪枝

对信息系统所面临的威胁进行合理的分类是准确赋值的前提。造成威胁的原因是多种多样的，可以大致分为**人为因素**和**环境因素**两大类。可以用下面这个“威胁树”来逐一细化各种威胁因素。需要向读者指出的是，这个威胁树并不是威胁分类的“百科全书”，仅是向读者展示进行威胁分类时惯用的分析方法和威胁举例。从图 8.1 所示的信息系统安全威胁树可以看出，在对威胁进行分类的时候，本质思想依然是考虑这些威胁对

信息系统的保密性、完整性和可用性等带来的潜在影响。

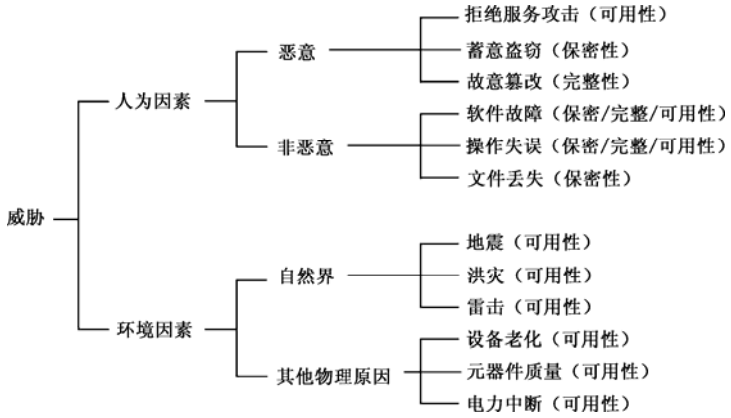


图 8.1　信息系统安全威胁树示意图

在实际从事威胁识别工作时，上面这种威胁树仅是一个进行威胁分类的“旅游路线图”。需要把它“文档化”，这一文档化的结果是威胁识别文档的组成部分（详见 8.3.2 节的有关威胁识别报告）。

常言道“事出有因”。在进行威胁分类之前，首先需要弄清楚产生威胁的“土壤”，即威胁起因。表 8.1 是撰写威胁分类文档时针对“环境因素、人员因素”进行的分析。



“威胁树”、“故障树”等是人们进行分类分析时最常用的方法之一。虽然原始，但却有效。不同的组织可以根据其实际情况绘制自身的威胁树，就如同生物工程学中绘制的基因图谱一样，这是一个非常烦琐、细致的“针线活”。然而，要做到“既见树木，又见森林”，要对这些“树干、树枝”进行关联分析，就需要从形式概念分析（FCA）、本体论（ontology）等方面进行探索。

表 8.1　威胁来源分类

来　源		描　述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通信线路等方面的故障
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益。外部人员利用信息系统的脆弱性，对网络或系统的保密性、完整性和可用性进行破坏，以获得利益或炫耀能力
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，或者没有遵循规章制度和操作流程而导致故障或信息损害；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击

接下来针对上面的威胁来源，可以根据其表现形式将威胁进行分类，如表 8.2 所示。

表 8.2　威胁分类

种　类	描　述	子　类
软、硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通信链路中断、系统本身或软件缺陷等	设备硬件故障、传输设备、存储媒体故障，系统软件故障，应用软件故障、数据库软件故障，开发环境事故等
物理环境影响	对信息系统正常运行造成影响的物理环境或自然灾害	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等
无所作为或操作失误	应该执行而没有执行相应的操作，或无意执行了错误的操作	维护错误、操作失误等
管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等
恶意代码	故意在计算机系统上执行恶意任务的程序代码	病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等
越权或滥用	通过采用一些措施，超越自己的权限访问本来无权访问的资源，或之后滥用自己的权限，做出破坏信息系统的行为	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等
网络攻击	利用攻击工具和技术通过网络对信息系统进行攻击和入侵	网络探测和信息采集、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等
物理攻击	通过物理的接触造成对软件、硬件、数据的损害	物理接触、物理破坏、盗窃
泄密	信息泄露给不应该了解的他人	内部信息泄露、外部信息泄露等
篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息，篡改用户身份信息或业务数据信息等
抵赖	不承认收到的信息和所做的操作和交易	原发抵赖、接收抵赖、第三方抵赖等

需要指出的是，上面这些指导性分类表格，在实际应用中要根据具体情况加以细化。读者将在 8.3 节案例分析中体会其应用的灵活性。



在“种植”了威胁树之后，下一步工作是对其进行“剪枝”，或者说量体裁衣：并不是所有威胁均需要加以考虑。例如，被评估单位地处内地，那么就无须考虑台风对信息系统带来的威胁。又如，被评估单位是一个与 Internet 隔离的业务内网，就无须考虑来自于 Internet 的拒绝服务攻击（DDOS）威胁。剪枝的另外一层含义是对于那些有可能存在的威胁，则需要尽量细化。例如，一个对外提供服务的数据中心，需要考虑的威胁既有供电方面的物理环境威胁，又有来自设备故障和人为攻击的威胁等。而在供电方面，又可以进一



宇宙飞船孤悬太空，与地球上的 Internet 似乎毫无瓜葛。然而最近美国太空站却遭受了 Gammina.AG 病毒的攻击，该病毒曾多次尝试盗取密码，使得 NASA 的计算机专家们忙乎了好几天，后来才查明罪魁祸首是宇航员自带的没有安装任何杀毒软件的笔记本电脑。

步细分为受雷电威胁影响和用电高峰季节电网跳闸的威胁等。来自设备故障的威胁则可以分为人为操作失误（错误地移开了正在传输信息的连接跳线）和同轴电缆或光纤被盗（很不幸，这也是偶尔发生的），来自人为的攻击则可以分为 DDOS 攻击（由于数据中心的重要性，DDOS 攻击对实时数据传输的威胁是致命的）、网络蠕虫、特洛伊木马（数据中心所存储的数据本身就对攻击者富有诱惑力）等。接下来还需要对 DDOS 攻击进一步细分，分析哪些是近来比较流行的 DDOS 攻击方式，同样对蠕虫、特洛伊木马等也需要“顺藤摸瓜”……

有的读者可能会感到疑惑，即使不考虑自然环境带来的威胁，规模如此庞大的虚拟空间的威胁怎样才能有效地进行分类呢？其实从根本上说，任何一个信息系统所面临的虚拟空间的威胁起因有两方面，一是攻击者所拥有的资源和技能，即这些攻击者本身是“业余爱好者”，商业间谍还是有庞大利益集团支持的有组织的黑客（群体），甚至是有战役战术目的的敌对网军。二是信息系统本身的吸引力。由于 Internet 的普及，现在众多的攻击工具和攻击技术可以轻易地从网上获取，因此不能简单地盲从国际上对威胁识别的流行观点，即首先考虑攻击者所能调动的资源和能力，而是应该首先考虑自己信息系统的价值，也就是说对潜在入侵者的吸引力有多大。从理论上来讲，如果您的信息资产具有“足够的”吸引力，那么您将面临的是来自全球的攻击威胁。所以人们也常说“知己胜于知彼”。在此基础上，再结合目前国际上流行的攻击方式进行威胁识别。因此归根到底，**资产识别的结果是进行威胁识别的出发点和落脚点。**这就是上面讲的对威胁进行分类的时候要量体裁衣的含义。

最后要提醒读者注意的是，在完成了量体裁衣式的威胁分类之后，应该将其整理成一个完整的威胁清单（见 8.3 节案例分析），这是威胁识别工作的一个必需的输出文档。

8.2.2　威胁赋值——统计

对威胁进行了分类识别之后，将进一步对这些威胁进行“定量”刻画，也就是**威胁赋值**。请读者回忆一下在第 7 章“资产识别”中的赋值方法。资产赋值是“自定义”的，也就是说组织根据对自身资产重要性的认识，在评估人员的协助下来“定价”。而威胁赋值则不同，它的基本指导思想是“它定义”，或者说是“客观定价”。



威胁赋值的依据是对各种威胁发生的频率进行统计。请读者记住，使用威胁树或者威胁分类（植树和分枝）的目的是“层层剥茧”，希望能够将抽象的、定性的威胁描述转化成可以定量分析的威胁。举例而言，在分析“威胁/环境因素/软件故障”（见表 8.2）这个



威胁分类仅仅能够起到“常见威胁”分析的作用。在信息系统越来越复杂，人–机结合越来越密切的今天，人们不可能对所有威胁形式都提前进行精确的预测。解决之道是建立应急响应与灾备体系（见本书第 11 章）。

威胁子类的时候，如何将“软件故障”与定量分析相结合呢？我们可以采用已经较为成熟的“软件可靠性标准”中的有关技术指标，如平均故障率（MTF）等。这样的数据可以从软件提供商出具的，并由独立第三方测试机构提供的该软件测试报告等技术资料中获得。同样的，在分析“威胁/人为因素/恶意人员/可用性破坏”这个威胁子类的时候，就可以根据防火墙或者 IDS 所记录的入侵频率来判断。

但是有很多威胁因素目前很难用数学公式表达出来。即使是上面提到的人为蓄意破坏的威胁，入侵者往往会采用对预先选择的目标进行“散乱扫描”的方式，一来进一步收集拟入侵的目标的信息，二来防止被防御系统记录其攻击规律，总之，这时候牵涉到不同攻击者的攻击行为。如果仅仅是使用诸如 IDS 日志来分析出现的频率，就远远不够了。因此，还需要运用自己的经验进行判断。

在进行威胁识别的时候，需要综合考虑以下 3 个方面内容来计算对具体组织信息系统所面临的各种威胁的频率。

（1）**历史记录：**以往安全事件报告中出现过的威胁及其频率的统计。这时需要测评人员针对资产的价值和安全事件报告中的威胁方式进行联动分析。例如，重要的数据库系统要重点关注针对数据安全的威胁，有无进行缓冲区溢出的攻击迹象（这类攻击一般将导致权限提升，从而能够对敏感数据进行任意操作）及频率是多少等；有无猜测口令的攻击痕迹及频率是多少等。

（2）**现场取证：**实际环境中通过检测工具及各种日志发现的威胁及其频率统计。读者可能会发现，目前不少被测评单位尚无比较完整和系统的安全事件报告。因此，通过检测工具和查看各种日志这种“现场取证”的工作就显得非常必要。当然，日志分析的出发点依然是资产本身的价值是否和日志中所发现的威胁痕迹有直接关联。下面的日志分析辅助工具可以协助测评人员进行相关的安全日志分析。

Sniffer 协议分析工具。估计大多数读者都听说过这款由 NAI 公司开发的嗅探工具。它是目前使用最普遍的嗅探工具之一，可广泛用于网络流量分析、协议分析和网络监控等领域。

逆火 IIS 日志分析工具。这款工具可以通过统计服务器日志，产生多种图表，其中还带有三维统计图。通过这些统计可以知道：有多少访客访问了此网站，有多少访客浏览了网站，访客都从哪里来，他们访问了哪些页面，哪些页面被忽略了及访客在网站停留了多长时间。该工具支持自动日志分析，具有计划器（schedule），可设置在服务器上自动运行。

（3）**权威发布：**近一两年来国际国内权威组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警报告。国际国内有众多的权威组织定期发布一些

造成重大影响的威胁报告，如美国的 CERT/CC、FIRST、SANS、中国的 CNCERT 等。这些权威组织提供的报告仅仅是起参考作用，评估人员需要根据正在评估的信息系统的实际情况来决定其作用。例如，对于一个 UNIX 系统占主体地位的信息系统，CERT 组织发布的有关 Windows 的威胁报告用处就不大。

与资产识别类似，在对威胁进行赋值的时候，也是采用分级的方式，如表 8.3 所示。

表 8.3　威胁赋值

等　级	标　识	定　义
5	很高	出现的频率很高（如：≥1 次/周）；或在大多数情况下几乎不可避免，或可以证实经常发生过
4	高	出现的频率较高（如：≥1 次/月）；或在大多数情况下很有可能发生，或可以证实多次发生过
3	中等	出现的频率中等（如：≥1 次/半年）；或在某种情况下可能会发生，或可以证实曾经发生过
2	低	出现的频率较小；或者一般不太可能会发生，或没有被证实发生过
1	很低	威胁几乎不可能发生，仅可能在非常罕见或例外的情况下发生

8.3　威胁识别案例分析

在本节中，将继续以“数字兰曦”为例，介绍如何进行威胁识别及该过程结束后应该输出的技术报告。

回忆在第 7 章进行资产识别的时候，将“数字兰曦”的资产分为了“信息环境、公用信息载体、专用信息及信息载体”三大类。因此，在下面进行威胁识别的时候，也将按照对应的资产分类方式并结合 8.2 节所描述的威胁分类方法，来对“数字兰曦”的信息环境资产、公用信息载体资产和专用信息及信息载体资产面临的威胁进行识别。

8.3.1　“数字兰曦”威胁识别

1.“数字兰曦”威胁源概述

在 8.2 节已经介绍过，对于信息系统而言，威胁来源大体上可以分解为环境因素和人为因素两大类（见 8.2 节“威胁树”），其中环境因素（自然灾害、设备老化等）造成的威胁是传统威胁，而人为因素给信息系统带来的威胁是“非传统”威胁。尽管人们经常遭遇的如病毒等安全威胁是发生在虚拟空间当中，并且以软件这种形式出现。但在这些威胁背后，实际上仍然是人的因素。至今为止，尚未发现有任何信息系统自动衍生出病毒软件出来。因此，在下面的案例分析中，无论是信息环境资产、公用信息载体资产还是专用信息及信息载体资产，均把人为因素作为威胁来源的主体加以考虑。

人为威胁因素可以继续细分为“无关的外部人员”（如黑客等）、合作第三方人员

（如委托开发软件的人员、风险评估人员等）、内部有意破坏人员和内部无意破坏人员（如误操作）。在对整个“数字兰曦”进行威胁识别的过程中，均是按照这个方法来分类的。顺便指出的是，为了节省篇幅，本书将威胁分类与赋值合并在一起。

1）信息环境威胁识别——软环境威胁

从系统科学的角度来讲，对无人参与的系统施加影响称为控制，对有人参与的系统施加影响称为管理。信息系统是最典型的“人–机合一”系统，信息系统的安全管理体系是系统发挥正常作用的组织保障。因此，管理体系本身也就自然纳入了进行威胁识别的范畴。管理体系包括人员和管理制度威胁识别两大类。

（1）人员资产威胁识别。

在第 7 章进行人员资产识别的时候曾经说过，由于兰曦公司最核心的信息化人员主要集中在公司的信息化领导小组和信息中心这两个部门当中，所以他们是最重要的人员资产，而分公司和研究院的人员资产重要性相对较低。那么，在进行威胁识别的时候是否只需对这两个部门的人员所面临的威胁进行识别，就能代表整个兰曦公司人员资产所面临的全部威胁了呢？显然不是。因为这两个部门的人员是整个“数字兰曦”的管理者，而“数字兰曦”还包括众多的使用者。因此，需要对兰曦公司信息化领导小组、信息中心及分公司/研究院（包括全国 145 个销售网点人员）这三大类人员资产面临的威胁进行识别。

在信息系统当中，自然环境对人员资产造成的威胁是非常低的（如果是考虑建筑安全风险，这就变成一个重要因素了）。那么信息系统之中人与人之间的威胁表现形式主要是什么呢？主要表现在欺骗威胁、窃密和权限滥用等几个方面。表 8.4 是我们与兰曦公司信息中心人员共同罗列的威胁清单和对威胁严重程度的赋值。

表 8.4　人员威胁严重程度赋值

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 附 值
1	公司信息化领导小组	环境因素	自然环境	1
		无合作的外部人员	欺骗威胁	3
			窃密	3
			权限滥用	2
		合作的第三方人员	欺骗威胁	3
			窃密	3
			权限滥用	3
		无意识破坏内部人员	欺骗威胁	1
			窃密	1
			权限滥用	1
		有意识破坏内部人员	欺骗威胁	3
			窃密	3
			权限滥用	3

续表

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 附 值
2	信息中心	信息环境	自然环境	1
		无合作的外部人员	欺骗威胁	2
			窃密	2
			权限滥用	2
		合作的第三方人员	欺骗威胁	2
			窃密	2
			权限滥用	2
		无意识破坏内部人员	欺骗威胁	1
			窃密	1
			权限滥用	1
		有意识破坏内部人员	欺骗威胁	2
			窃密	2
			权限滥用	2
3	分公司/研究院人员	信息环境	自然环境	1
		无合作的外部人员	欺骗威胁	1
			窃密	1
			权限滥用	1
		合作的第三方人员	欺骗威胁	1
			窃密	1
			权限滥用	1
		无意识破坏内部人员	欺骗威胁	1
			窃密	1
			权限滥用	1
		有意识破坏内部人员	欺骗威胁	1
			窃密	1
			权限滥用	1

（2）管理制度威胁识别。

显然，兰曦公司制定的各种管理制度不会面临自然灾害的威胁（或者说这种威胁发生的可能性微乎其微），我们依然考虑的是人为的威胁，如表 8.5 所示。

表 8.5　管理制度威胁严重程度赋值

资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 附 值
信息化规章管理制度	无合作的外部人员	信息探测威胁	4
		窃密威胁	3
	合作的第三方人员	信息探测威胁	3
		窃密威胁	3

续表

资产名称	威胁来源	威胁种类	威胁附值
信息化规章管理制度	无意识破坏内部人员	权限滥用	3
		泄密	4
	有意识破坏内部人员	信息探测威胁	4
		窃密威胁	4
		权限滥用	4

在表 8.5 中罗列出了“信息探测威胁”这个子类。事实上有些组织机构（如政府部门）的内部管理规章制度是比较敏感的，一旦泄露就有可能给有心人寻找管理制度的漏洞提供机会。

2）信息环境威胁识别——硬环境威胁

作为整个信息系统运行的基础及物理上的最外围保护措施，机房及保障设备本身的安全也是一个需要重点关注的地方。作为一个客观存在的物理实体，机房及保障设备的安全受到多种途径的威胁，包括自然环境的威胁、支撑环境（机房建筑质量等）的威胁、人员的威胁。

“数字兰曦”由于系统的分布覆盖面较广，机房建设的情况也较为复杂，作为整个系统主要机房的公司中心机房和分公司/研究院机房是分别按照国家 A、B 两类机房建设标准进行建设的，机房选址时充分考虑了巴山市的地质灾害情况，配备了较为完善的保障设备和门禁设施，并在系统长期的运行维护中制定了较为完备的相关管理制度等。但在公司信息中心机房的运行中曾出现过机房断电的情况，因此在有良好基础设施及较完备的管理制度条件下，仍然需要对机房及保障设备进行威胁分析。此外，对于机房的网络拓扑结构等信息，也应当是属于一个组织高度关注的保密内容。因此，需要考虑“泄密”的威胁。

机房及保障设备威胁分类及其严重程度赋值如表 8.6 所示。

表 8.6　机房及保障设备威胁分类及其严重程度赋值

序号	资产名称	威胁来源	威胁种类	威胁附值
1	公司信息中心机房	信息环境	自然环境	1
			系统支撑环境	2
		无合作的外部人员	系统物理设备未授权访问	1
			窃密	1
		合作的第三方人员	系统物理设备未授权访问	2
			窃密	3
		无意识破坏内部人员	系统物理设备未授权访问	1
			误操作	2
			泄密	1
		有意识破坏内部人员	系统物理设备未授权访问	2
			泄密	4

续表

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 附 值
2	分公司/研究院机房	信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	1
			窃密	2
		合作的第三方人员	系统物理设备未授权访问	2
			窃密	2
		无意识破坏内部人员	系统物理设备未授权访问	1
			误操作	2
			泄密	1
		有意识破坏内部人员	系统物理设备未授权访问	2
			泄密	3

2．公用信息载体威胁识别

公用信息载体资产包括通信设备和安全防护设备等，它们面临的威胁如下所述。

1）通信设备威胁识别

控制核心路由器/交换机，或者对其发起拒绝服务攻击，窃取这些核心网络设备的配置信息等，是常见的安全威胁之一。因此，在威胁识别中增加了若干与此相关的威胁子项，如表 8.7 所示。

表 8.7　通信设备威胁严重程度赋值

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 附 值
1	三层交换机 CISCO 6506	信息载体故障	设备硬件故障	4
			网络操作系统故障	5
		信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	4
			系统资源未授权访问	5
			拒绝服务威胁	5
		合作的第三方人员	系统物理设备未授权访问	1
			系统资源未授权访问	2
		无意识破坏内部人员	系统物理设备未授权访问	4
			误操作	5
			泄密	5
		有意识破坏内部人员	系统资源未授权访问	4
			拒绝服务威胁	4
			泄密	5
2	华为 3COM s5126	信息载体故障	设备硬件故障	2
			网络操作系统故障	3

续表

序号	资产名称	威胁来源	威胁种类	威胁附值
2	华为 3COM s5126	信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	2
			系统资源未授权访问	3
			拒绝服务威胁	4
		合作的第三方人员	系统物理设备未授权访问	2
			系统资源未授权访问	2
		无意识破坏内部人员	系统物理设备未授权访问	2
			误操作	3
			泄密	3
		有意识破坏内部人员	系统资源未授权访问	2
			拒绝服务威胁	2
			泄密	3
	……			

2）安全防护设备威胁识别

将安全设备当作攻击跳板或旁路迂回（by pass）是目前攻击者研究的热门领域之一。因此，在针对“数字兰曦”安全防护设备的威胁识别中，威胁子项的分类就新增了包括“修改访问控制策略”、“篡改安全日志”等常见的攻击行为，如表 8.8 所示。

表 8.8　安全防护设备威胁严重程度赋值

序号	资产名称	威胁来源	威胁种类	威胁附值
1	天融信防火墙 4000V2	信息载体故障	设备硬件故障	4
			网络操作系统故障	5
		信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	4
			系统资源未授权访问	5
			拒绝服务威胁	5
		合作的第三方人员	系统物理设备未授权访问	2
			系统资源未授权访问	2
		无意识破坏内部人员	系统物理设备未授权访问	4
			误操作	5
		有意识破坏内部人员	系统资源未授权访问	4
			修改访问控制策略	4
			篡改安全日志	5

续表

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 附 值
2	美国 FortiGate 防火墙 1000A	信息载体故障	设备硬件故障	2
			网络操作系统故障	3
		信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	2
			系统资源未授权访问	3
			拒绝服务威胁	3
		合作的第三方人员	系统物理设备未授权访问	2
			系统资源未授权访问	2
		无意识破坏内部人员	系统物理设备未授权访问	2
			误操作	3
			泄密	3
		有意识破坏内部人员	系统资源未授权访问	2
			修改访问控制策略	2
			篡改安全日志	3
3	联想网御防火墙 POWER-V 404	信息载体故障	设备硬件故障	2
			网络操作系统故障	3
		信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	2
			系统资源未授权访问	3
			拒绝服务访问	2
		合作的第三方人员	系统物理设备未授权访问	2
			系统资源未授权访问	2
3	联想网御防火墙 POWER-V 404	无意识破坏内部人员	系统物理设备未授权访问	2
			误操作	3
		有意识破坏内部人员	系统资源未授权访问	2
			修改访问控制策略	2
			篡改安全日志	3
4	北京中科网威防火墙 NETPOWER	信息载体故障	设备硬件故障	2
			网络操作系统故障	3
		信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	2
			系统资源未授权访问	3
			拒绝服务威胁	2
		合作的第三方人员	系统物理设备未授权访问	2
			系统资源未授权访问	2

续表

序号	资产名称	威胁来源	威胁种类	威胁附值
4	北京中科网威防火墙 NETPOWER	无意识破坏内部人员	系统物理设备未授权访问	2
			误操作	3
		有意识破坏内部人员	系统资源未授权访问	2
			篡改安全日志	2
			修改访问控制策略	3
5	中联绿盟“冰之眼”IDS 1600D	信息载体故障	设备硬件故障	4
			网络操作系统故障	5
		信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	系统物理设备未授权访问	4
			系统资源未授权访问	5
		合作的第三方人员	系统物理设备未授权访问	2
			系统资源未授权访问	2
		无意识破坏内部人员	系统物理设备未授权访问	4
			误操作	5
		有意识破坏内部人员	系统资源未授权访问	4
			修改访问控制策略	4
			篡改安全日志	5
	……			

3．专用信息及信息载体威胁识别

“兰芯”子系统是“数字兰曦”中最重要的一个子系统，其责任是：通过供应商管理终端，采集客户订单信息；根据客户订单信息，一方面产生电子结算信息与银行进行电子结算，另一方面对电子结算成功的订单信息通过数字仓储子系统（WMS）产生配送订单及配送，电子结算不成功的返回到供应商管理系统通知客户重新进行结算。

因此，“兰芯”子系统是兰曦公司业务处理的核心，在所有资产中属于最重要的部分，它的运行情况是否正常直接关系到兰曦公司的日常工作能否正常进行，如遇到问题将会导致严重的后果。

在这个子系统中，主要使用的硬件设备分别是一对互为热备（Hot standby，指主机出现故障时备份机立即接替主机的工作）的 IBM P550 小型机，一台与银行进行结算的 IBM PC 前置机，一台 IBM X346 测试机和两个 FAST T600 磁盘阵列。配置的软件分别采用的是 Aix 5.3，数据库软件是 DB2。

“兰芯”子系统的服务器操作系统主要是 Aix 5.3，经使用漏洞扫描设备进行检查，发现该操作系统存在高危漏洞，从而导致整个子系统出现漏洞，同时，管理子系统数据的 DB2 数据库出现配置问题，也对“兰芯”子系统产生威胁。



软件故障属于人为失误这一类威胁。无论是操作系统还是应用软件的高故障率给信息系统带来的威胁都不容轻视。法国“阿丽安娜”运载火箭发射失败、美国“火星登录者”宇宙飞船着陆时坠毁，事后查明的原因均属于应用软件编程过程中的人为疏忽，但这一念之差却给欧洲宇航局和 NASA 带来了巨大的损失。

在对“兰芯”子系统的专用信息及信息载体进行威胁识别的时候，根据这些专用信息及信息载体所承载的业务重要性（也就是资产重要性），新增了如数据篡改、恶意代码、权限滥用等新的威胁形式。公用信息载体其实也从某种程度上面临这些威胁，但根据“数字兰曦”网络拓扑结构，上述威胁一旦成为事实，对“数字兰曦”核心业务的载体——“兰芯”子系统的破坏力更大，所以将这些威胁识别放入到专用信息和信息载体这部分。此外，细心的读者也许已经发现在“合作第三方人员”的威胁子项中有一项赋值较高，即“软件故障”类。这是因为该项威胁对应的是软件开发商“快帆”公司在开发针对“数字兰曦”的业务开发的应用软件目前故障率（MTF）还比较高，因此在评估过程中对此加以了特别关注，如表 8.9 所示。

表 8.9　专用信息及信息载体威胁严重程度赋值

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 赋 值
1	“兰芯”子系统应用服务器、热备应用服务器和操作系统及应用软件	信息载体故障	主机操作系统故障	4
			信息载体硬件故障	4
			应用系统故障	3
		信息环境	自然环境	1
			系统支撑环境	1
		无合作的外部人员	信息探测威胁	4
			窃密威胁	4
			欺骗威胁	5
			拒绝服务威胁	5
			数据驱动攻击威胁	4
			数据篡改	4
			恶意代码	5
			系统资源未授权访问	4
		合作的第三方人员	信息探测威胁	3
			窃密威胁	2
			欺骗威胁	2
			拒绝服务威胁	1
			数据驱动攻击威胁	2
			数据篡改	3
			恶意代码	2
			系统资源未授权访问	2
			应用软件故障	4

续表

序号	资产名称	威胁来源	威胁种类	威胁赋值
1	“兰芯”子系统应用服务器、热备应用服务器及操作系统及应用软件	无意识破坏内部人员	恶意代码	4
			权限滥用	4
			泄密	4
		有意识破坏内部人员	信息探测威胁	4
			窃密威胁	4
			欺骗威胁	5
			数据驱动攻击威胁	4
			数据篡改	4
			恶意代码	4
			权限滥用	4
2	“兰芯”子系统数据库服务器、热备服务器及操作系统、数据库软件和应用软件	信息载体故障	主机操作系统故障	4
			信息载体硬件故障	4
			应用系统故障	4
		信息环境	自然环境	4
			系统支撑环境	5
		无合作的外部人员	信息探测威胁	5
			窃密威胁	5
			欺骗威胁	5
			拒绝服务威胁	5
			数据驱动攻击威胁	5
			数据篡改	5
			恶意代码	5
			系统资源未授权访问	5
		合作的第三方人员	信息探测威胁	2
			窃密威胁	2
			欺骗威胁	2
			拒绝服务威胁	2
			数据驱动攻击威胁	2
			数据篡改	3
			恶意代码	3
			系统资源未授权访问	3
			应用软件故障	4
		无意识破坏内部人员	恶意代码	5
			权限滥用	5
			泄密	5
		有意识破坏内部人员	信息探测威胁	5
			窃密威胁	5
			欺骗威胁	5
			数据驱动攻击威胁	5
			数据篡改	5
			恶意代码	5
			权限滥用	5

续表

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 赋 值
3	主机服务器——“兰芯”子系统前置机与各大银行通信进行实时电子结算的前置机及操作系统和应用软件	信息载体故障	主机操作系统故障	4
			信息载体硬件故障	4
			应用系统故障	4
		信息环境	自然环境	1
			系统支撑环境	5
		无合作的外部人员	信息探测威胁	5
			窃密威胁	5
			欺骗威胁	5
			拒绝服务威胁	5
			数据驱动攻击威胁	5
			数据篡改	5
			恶意代码	5
			系统资源未授权访问	5
		合作的第三方人员	信息探测威胁	2
			窃密威胁	3
			欺骗威胁	2
			拒绝服务威胁	2
			数据驱动攻击威胁	2
			数据篡改	3
			恶意代码	2
			系统资源未授权访问	2
			应用软件故障	4
		无意识破坏内部人员	恶意代码	5
			权限滥用	5
			泄密	5
		有意识破坏内部人员	信息探测威胁	5
			窃密威胁	5
			欺骗威胁	5
			数据驱动攻击威胁	5
			数据篡改	5
			恶意代码	5
			权限滥用	5
4	“兰芯”子系统前端测试机及操作系统	信息载体故障	主机操作系统故障	1
			信息载体硬件故障	1
			应用系统故障	1
		信息环境	自然环境	1
			系统支撑环境	2
		无合作的外部人员	信息探测威胁	4
			窃密威胁	4
			欺骗威胁	4
			拒绝服务威胁	3
			数据驱动攻击威胁	3
			数据篡改	4
			恶意代码	3
			系统资源未授权访问	3

续表

序号	资产名称	威胁来源	威胁种类	威胁赋值
4	“兰芯”子系统前端测试机及操作系统	合作的第三方人员	信息探测威胁	2
			窃密威胁	1
			欺骗威胁	1
			拒绝服务威胁	2
			数据驱动攻击威胁	1
			数据篡改	2
			恶意代码	1
			系统资源未授权访问	2
		无意识破坏内部人员	恶意代码	3
			权限滥用	2
			泄密	3
		有意识破坏内部人员	信息探测威胁	3
			窃密威胁	3
			欺骗威胁	3
			数据驱动攻击威胁	3
			数据篡改	4
			恶意代码	2
			权限滥用	4
5	磁盘阵列	信息载体故障	信息载体硬件故障	4
		信息环境	自然环境	4
			系统支撑环境	5
		无合作的外部人员	系统物理设备未授权访问	4
		合作的第三方人员	系统物理设备未授权访问	4
		无意识破坏内部人员	系统物理设备未授权访问	4
		有意识破坏内部人员	系统物理设备未授权访问	4
6	无线路由器 CISCO aironet 1200	信息载体故障	设备硬件故障	2
			网络操作系统故障	3
		信息环境	自然环境	2
			系统支撑环境	3
		无合作的外部人员	系统物理设备未授权访问	2
			系统资源未授权访问	3
		合作的第三方人员	系统物理设备未授权访问	2
			系统资源未授权访问	2
		无意识破坏内部人员	系统物理设备未授权访问	2
			误操作	3
			泄密	3
		有意识破坏内部人员	系统资源未授权访问	2
			泄密	3

续表

序号	资 产 名 称	威 胁 来 源	威 胁 种 类	威 胁 赋 值
7	“兰芯”子系统专用 IP 地址资产	无合作的外部人员	信息探测威胁	5
			窃密威胁	4
		合作的第三方人员	信息探测威胁	2
			窃密威胁	2
		无意识破坏内部人员	权限滥用	4
			泄密	5
		有意识破坏内部人员	信息探测威胁	5
			窃密威胁	4
			权限滥用	4
	……			

至此，我们完成了对“数字兰曦”信息环境、公用信息载体及专用信息和信息载体所面临的威胁识别，以及对威胁严重程度的赋值工作。

8.3.2　威胁识别输出报告

与第 7 章类似，威胁识别结束之后也需要出具《威胁识别技术报告》。该报告的主体包括被评估单位面临的威胁概述、威胁分类和对威胁严重程度的赋值等。下面仍以“数字兰曦”为例给出该报告的格式，仅供参考。

“深海”信息安全测评中心

“数字兰曦”威胁识别技术报告

摘要

目录

图标目录

报告审批（授权签字）及日期

1　撰写依据

2　术语解释

3　威胁分类原则和方法

错误！4　“数字兰曦”系统威胁概述

5　“数字兰曦”威胁识别

5.1　“兰芯”子系统威胁识别

5.2　“兰剑”子系统威胁识别

5.3　……

6　附录

8.4　本章小结

- 威胁的概念
- 威胁识别的概念
- 重点识别与全面识别
- 威胁分类与威胁树
- 威胁赋值
- 威胁识别报告

尾声：在鹰隼盘旋的天空下

蓝天，雪峰，丛林，奔逃的雪兔，俯冲的鹰隼。

除了食物链的顶端，大量的动物都生活在其天敌的威胁之下。

自从人类凭借其优越的大脑成为世界的主宰之后，他的各类“天敌”就已万劫不复。

人类早已脱离了那个弱肉强食的食物链。人类甚至要保护那个食物链中的一切生灵，哪怕它是处于那个食物链的顶端。强大到一定的程度，就有（才有）了与世无争的资格。

本来，这样的世界就该像天堂般美丽了。但是……

但是，人类受到的威胁却从未消失过。而且，似乎永远不会消失殆尽。

谁在威胁人类？除了不可抗力的大自然，那就是——人类自身。

既然威胁将永远存在，就只有让我们自身变得更加强盛。所以，让水里有狂鲨游弋，让林中有野虎出没，让天上有猛禽盘旋……

观感

（1）试举例说明哪些威胁是现实社会具有的，但它们却不是目前信息安全威胁识别的重点。哪些威胁是信息系统具有的，但对现实社会还不足以构成威胁？

（2）以您所在单位门户网站（如校园门户网站）为例，画出该网站的“威胁树”。

（3）在网上下载并在您自己的计算机上安装 Sniffer 等嗅探工具，然后提交使用报告。

（4）在网上下载并试用常用的日志分析软件，如“逆火 IIS”、eWebblog Analyzer 等，然后配置在本单位（如本校/本学院）的 Web 服务器上，运行一周之后给出你对这几款工具的使用意见。

（5）CMM/CMMI 是国际软件界对软件企业质量认证的一种常用方式。如果您的信息系统要求软件平均故障率是 15%/年以下，请问您会选择 CMM/CMMI 几级以上的软件

企业参与您所在单位信息系统的建设?

（6）打开您自己的计算机查看近一周的安全日志或系统日志，并分析您所面临的安全威胁频率。

（7）请查阅 CNCERT 本月主要安全威胁报告。

（8）请在本章案例分析的基础上完成《“兰芯”子系统威胁识别技术报告》。

（9）请在第 7 章最后“观感”部分中对“杜甫”子系统资产识别的基础上，对其进行威胁识别，并按照本章所建议的威胁识别技术报告内容出具《杜甫子系统威胁识别技术报告》。

第 9 章

脆弱性识别





阿基里斯雕塑

千丈之堤，以蝼蚁之穴溃；百尺之室，以突隙之烟焚。

——韩非《韩非子·喻老》

序幕：永恒的阿基里斯之踵

提起脆弱性，人们最容易想到的大概就是古希腊那位战神的脚踵（Achilles' Heel），它是英雄身上唯一的、但却众所周知而且致命的漏洞。

今天的漏洞，却可能是“敌知我不知，我知敌不知”，甚至是“敌我暂时都不知”。双方博弈的目标就是看谁成为“先知”。

1957 年 10 月 4 日，前苏联拜拜努尔发射场。一枚用洲际导弹临时改装的运载火箭腾空而起，将一颗比篮球稍大一点的金属球送上了太空，人类的使者第一次叩响了上帝的大门！然而，这位芳名与诗歌一样优雅的人造天体——“地球伴侣号”（Sputnik）不停发射的无线电波给美国人带来的却不是爱侣的秋波，而更像是一场噩梦，因为这个伴侣每隔 1.5 小时就会从高傲的美国人头顶上飞过，“山姆”大叔有一种连总统卧室都被赫鲁晓夫主席一览无遗的尴尬和惊慌。“亡羊补牢”，在艾森豪威尔总统的指示下，1958 年美国国防部成立了国防部高级研究计划署（DARPA），它当初的宗旨是应对前苏联来自太空的威胁，然而这位总统先生可能做梦都没有想到，10 年后 DARPA 会生下一个可以与 Achilles 媲美的神童——Internet。

1988 年，23 岁的 Morris 懵懵懂懂地向 Internet 的脚踵投出了第一支标枪……尽管 FBI 至今没有正式公布其源代码，但可以肯定的是，Morris 当初所发现的，也是今天众多黑客不停寻找、利用和享受的以 TCP/IP 这个君子协议（Gentlemen Agreement）为代表的网络协议的安全漏洞。

要点：本章结束之后，读者应当了解和掌握

- 脆弱性和资产是什么关系？
- 脆弱性识别包括哪些内容？
- 怎样进行脆弱性分类与赋值？
- 如何撰写脆弱性识别报告？

9.1　脆弱性概述

本节将介绍风险评估的第三个环节——**脆弱性**及**脆弱性识别**。脆弱性是资产本身的固有属性，任何资产都有其脆弱性。从哲学的观点来看，任何事物都有其正反两方面的属性，否则就是一个“怪胎”。甚至同一事物的“坚固性”与“脆弱性”这一对矛盾也是可以在一定条件下相互转化的。例如，冷战结束后，特别是“海湾战争”的大获全胜，使得美国的科技实力、军事实力等达到了顶峰，给人一种坚不可摧的印象。然而本・拉登的徒弟们却偷偷溜到纽约和华盛顿，将民航客机残忍地变成了“神风敢死队”，又让人感叹美利坚合众国内部处处是漏洞；又例如，拒绝服务攻击等屡见不鲜的安全事件带来的网络阻塞，使得人们认为 Internet 是弱不禁风的，但在“5.12”汶川大地震中（按照地震级别的分类，8.0 级属于毁灭性地震），当所有的电话都是一片盲音的时候，却从震中地区阿坝州政府网站传来了求救的信息……

现在来看一看信息系统脆弱性的定义。



脆弱性（vulnerability），指可能被威胁所利用的资产或若干资产的薄弱环节。

下面几个与脆弱性相关的概念可以帮助读者加深对脆弱性的理解。

1．绝对和相对

既然脆弱性是资产的固有属性，那么只要有资产就有脆弱性。从这个角度来讲脆弱性是绝对的。但这并不意味着绝对存在的脆弱性一定会带来安全事件，如在第 7 章里提到的不会游泳的人与生活在沙漠中的关系那个例子。另一方面，在互联网时代，人们可以非常方便地获取所需要的资源。因此，针对某种脆弱性的利用方法很快就会遍及全球，如现在所谓的“零日攻击”（Zero-day attack）使得脆弱性被威胁所利用的时间越来越短。因此，在虚拟空间中，人们是在不停地与攻击者赛跑，力争在被有心人利用之前弥补自身的脆弱性。



2005 年 12 月 27 日，人们发现微软的 WMF 影像处理功能出现重大安全漏洞，虽然微软在翌日发布了有关该漏洞的安全性摘要报告，但直到 2006 年 1 月 10 日才公布漏洞的修正补丁。而实际上，Internet 上针对该漏洞的攻击程序在漏洞被发现的同一天就出现了。尽管微软等大型 IT 巨头后来纷纷与各个知名的安全服务机构（如 CERT 等）签署了协议，在他们发布补丁之前请这些安全机构不要公布任何漏洞信息，但遗憾的是，全世界的黑客也在夜以继日地工作，因为对当代许多黑客而言，漏洞就是金钱……

2．技术和管理

提起脆弱性，读者最容易想到的大概就是 Windows 操作系统上的各种漏洞等技术层

面的概念。这毫无疑问能帮助我们理解什么是脆弱性。但实际工作中，往往有一大部分关于脆弱性的内容没有引起人们足够的重视，那就是“管理脆弱性”。管理脆弱性有很多种，但大体上可以分为两类：一类是**结构脆弱性**，即信息安全管理体系不完备。例如，一个组织的信息系统只有安全管理员岗位，没有安全审计员岗位等。第二类是**操作脆弱性**，“在其位不谋其政”，各种管理制度虽然完整，但并没有真正得到贯彻执行。例如，很多单位都制定了应急预案，但并没有真正去检验预案的可操作性。在实际评估过程中，一个单位往往既存在结构脆弱性，也存在操作脆弱性。

3．点和面

“漏洞”是人们描述一个系统存在弱点的最早的用词，它给人的感觉是刚性、离散或者说是“点状”的。由于系统复杂性的缘故，人们现在越来越意识到应该用柔性、连续、或者说是“面上”的词语来描述系统的这个特征属性。因此，越来越多的人们采用了“脆弱性”这个词，本书也将采用这个术语。

寻找、分析和度量脆弱性，是风险评估中最重要，也往往是最困难的环节。下面首先给出脆弱性识别的定义。



脆弱性识别（vulnerability recognition），指分析和度量可能被威胁利用的资产薄弱环节的过程。

毫无疑问，脆弱性识别的立足点就是资产识别结果，否则识别工作就是“无本之木、无源之水”。脆弱性识别也分为“重点识别”和“全面识别”，其原理和第 8 章“威胁识别”相同，这里不再赘述。脆弱性可以分为“显形”和“隐形”两种。前者包括权威机构已经公布的操作系统漏洞等，比较容易发现。后者只有在一定环境和条件下才会显现出来，因此需要从系统科学的角度来认识。

9.2　脆弱性识别的诸方面

与资产识别和威胁识别略有不同，脆弱性识别分为**脆弱性发现、脆弱性分类、脆弱性验证**和**脆弱性赋值** 4 个环节。下面分别阐述其含义。

9.2.1　脆弱性发现

与资产和威胁不同，脆弱性识别的第一步是根据每一个具体的资产来寻找其脆弱性。例如，在评估过程中，针对某个单位信息系统所采用的操作系统版本型号，通过各种漏洞扫描设备来发现其脆弱性。这些扫描设备均能输出被扫描对象的各种脆弱性信息。这是发现系统脆弱性最常用的方法之一。但根据我们的经验，读者在进行脆弱性发现的时候要注意以下问题。



（1）**谨慎挑选扫描工具**。目前有各种流行的脆弱性扫描工具，对初学者而言，Nesuss、X-Scan 等扫描软件是大家常用的工具之一。但要注意这些软件本身带有诸多攻击性渗透测试包，如果使用不当，在评估一个信息系统的安全隐患的同时，也可能给它带来了新的风险（还记得在第 8 章讲威胁识别的时候，对合作第三方人员的威胁赋值吗？）。一种方法是使用这些工具之前关闭那些带有攻击性、破坏性的测试选项及那些不明的选项；还有一种方法，就是采用那些通过了国家权威测评机构检测的专用扫描工具（值得一提的是，这其实也是转嫁风险的一种方式）。



Nessus 是一个功能比较齐全而又易于使用的远程扫描软件，它的主要功能是对指定网络进行安全检查，找出该网络是否存在安全隐患（CVE）。该系统被设计为 client/sever 模式，服务器端负责进行安全检查，客户端用来配置管理服务器端。在服务器端还采用了 plug-in（插件式）设计，允许用户加入执行特定功能的插件，从而使用户可以进行更快速和更复杂的安全检查。

（2）**多方验证扫描结果**。在条件允许的情况下，建议评估人员使用不同的扫描设备对同一对象，特别是那些对组织业务战略起到核心作用的信息资产进行扫描并对比其结果。不同的扫描工具设计思想有所不同或者在扫描结果输出方面有一些细微的差异，这些差异有助于测评人员从不同的角度来发现系统存在的安全隐患。



作为最早的信息安全专业服务机构，CERT 在发布 CVE 信息方面具有很大的影响力，甚至有人将 CERT 称为 CVE 的“麦加圣地”（The Mecca of CVE）。但近年来关于 CERT 的作用也逐步引起了大家的争议。特别是它有可能在 CVE 信息发布方面的片面性和选择性等方面值得人们进一步观察。此外，随着中国 IT 企业的影响力逐步上升，一些国内企业生产的设备 CVE 信息也成为我们关注的焦点……

（3）**不要盲从扫描结论**。在许多情况下，扫描工具会出具“海量”的扫描结果，特别是使用者启用了所有扫描选项的时候（作者认为有部分扫描工具设计者是采用“宁可错杀一千，也不漏掉一个”的思想来设计自己大而全的软件的，以免漏掉漏洞而被同行耻笑）。面对这些扫描结果，测评人员应当用“怀疑”的态度去科学地对待。换言之，这些输出结果是否真正代表被检测系统就真正存在这些令人眼花缭乱的脆弱性，需要进行实际验证。我们将在“脆弱性验证”这一节和本章后面的案例分析中予以阐述。

（4）**既要树木又要森林**。测评人员往往“满足”于发现各种操作系统，特别是 Windows 系统的 CVE，因为这方面的数据库最为全面。但是也要注意一个信息系统还包括由多家厂商提供的各种设备。在许多国际权威组织发布的 CVE 信息中，也包括了大量网络设备所存在的脆弱性信息。建议评估人员根据资产的实际情况（设备型号、软件版本等）来核查该资产是否存在相应的脆弱性。

总之，脆弱性发现是风险评估工作中“技术含量”最高的部分（即使是针对管理脆弱性的发现而言也是如此）。它需要测评人员逐步积累工程经验，并站在系统工程的角度来思考。

9.2.2　脆弱性分类

在发现了资产所具有的脆弱性的基础上，接下来自然就应该考虑对这些脆弱性进行分类。分类方法依然是我们已经熟悉的“树状模型”（或“礼花模型”）。只是要再次强调一下这个观点，即今天的信息系统，是一个“人–机合一”的复杂系统，在信息环境资产、公用信息载体资产和专用信息及信息载体资产中，实际上也可以分为技术资产（软、硬件设备，数据等）和管理资产（组织结构、人员等）。因此，根植于资产之上的脆弱性也分为“**技术脆弱性**”和“**管理脆弱性**”，如表 9.1 所示。

表 9.1　脆弱性分类

类　型	识 别 对 象	识 别 内 容
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别
	系统软件	从补丁安装、物理防护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别

与第 7 章和第 8 章类似，这个脆弱性分类表仅仅是在进行资产脆弱性识别时候的指导性分类表。评估人员应当结合组织的实际情况进行脆弱性分类识别。读者在本章后面案例分析中对此会有进一步的了解。

9.2.3　脆弱性验证

对于一个高质量的风险评估工作而言，在进行脆弱性发现的同时，实际上也需要对所采集的（现场调研、扫描等）脆弱性信息进行验证。脆弱性验证实际上牵涉的问题不仅是脆弱性的核查和落实，还包括更深层面的含义。下面是作者提供给读者的建议。



（1）**脆弱性的在线验证**。由于在测评工作中，被测评的对象往往是在线运行的关

键系统，所以对脆弱性验证工作要考虑到尽量不影响被测评单位信息系统的正常运行。测评人员可以选择被测系统不太繁忙的时候进行脆弱性验证（如夜晚、周末或长假的时候）。同时要注意验证之前要做好各种应急预案，特别是牵涉到核心业务数据的时候，要有备份恢复的方案。

（2）**脆弱性的仿真验证**。对于那些业务连续性很强的机构（如金融、电力等），建议测评人员选择仿真验证的方式。尽管仿真度越高，结果越可靠，但鉴于目前大多数测评机构的实际情况和昂贵的仿真环境搭建不是一朝一夕之工，所以可以选择那些对组织的业务既关键，同时又比较容易实现的仿真方案，如操作系统、数据库管理系统 CVE 的仿真验证等。仿真验证还有一个好处就是可以“放开手脚”地进行各种破坏性、渗透性测试，从而尽量发现这些 CVE 对被测评单位业务的影响。读者将在本章的案例分析中看到如何部署简单的仿真环境，对所发现的 CVE 漏洞进行仿真验证。

（3）**对待脆弱性的客观态度**。如果我们告诉读者，并不是所有（验证了的）脆弱性都需要加以关注，并不是所有漏洞都需要打上补丁，有的读者可能会暂时难以理解。其实这在评估工作中，特别是风险评估完成之后提出安全解决方案的时候往往会出现的情况。有的时候安装补丁之后尽管封堵了某个设备或软件的漏洞，但随之而来的是整个信息系统运行效率的急剧下降，因为尽快提供某个 CVE 的补丁仅仅是生产这个设备或软件的厂商关注的，他们并不了解也不关心会给其他设备带来什么潜在影响。这就是我们经常讲的要应用系统工程的思想来解决实际问题的道理。此外，有不少脆弱性可以通过系统整体的防御能力来予以化解，所以在处理这些实际问题的时候，需要测评工程师充分发挥创造能力和艺术想象力。

9.2.4　脆弱性赋值

为了科学地把握脆弱严重程度的大小，与前面讨论资产和威胁一样，最后要对脆弱性的严重程度进行赋值。赋值时应该从以下角度进行综合考虑。

（1）**脆弱性对资产的暴露程度**。所谓脆弱性对资产的暴露程度，从技术上比较容易理解。例如，某服务器存在弱口令漏洞，一旦被猜解破译就能轻松地控制这台设备，因此弱口令对该服务器的暴露程度就很高。同时也要指出另外一个层面的暴露，那就是管理体系中存在的“结构脆弱性”。这一脆弱性如果不及时加以封堵，会给整个信息系统带来高危风险。所以一旦在评估过程中发现了这类管理问题，就应该给予高度重视。事实上，国家有关测评标准中对一些关键的管理薄弱环节采用了“一票否决”制来说明有关部门对此的态度。

（2）**脆弱性利用的难易程度**。要成功利用该脆弱性，攻击者所需要具备的技术实力有多高？需要调动的其他相关的资源有多大？在前面已经介绍过，在 Internet 快速发展的今天，诸多技术、工具均可以在网络上获得。但这并非就意味着该脆弱性被利用的门槛就一定非常低。事实上，在一个管理制度非常完善的组织内部，即使“外面的世界很

精彩”，也能够有效地防御各种来自互联网的威胁。例如，目前通过传输介质进行木马、蠕虫等病毒的传递非常普遍，但是如果一个单位对核心设备、终端 PC 的 UBS 端口进行了有效监控和管理，就能很大程度上避免由此带来的损失。如果是这种情况，即使该脆弱性非常容易被利用，但给予它的赋值也可适当降低。因此，我们常常强调信息安全是“管理与技术并重”。

（3）**脆弱性的流行程度**。有些脆弱性是目前公认的“高危漏洞”（可从 CVE 数据库中查询），这说明该漏洞一旦被利用会给系统带来严重影响。因此，评估人员应当向被评估单位及时说明，并建议尽快进行处理。例如，核心服务器操作系统存在的缓冲区溢出漏洞，既可以通过及时下载补丁的方式，也可以通过调整外围安全防护设备的访问控制策略（如封闭利用该漏洞的通信端口）等方式予以解决。但在解决之前，应当对该脆弱性严重程度赋予较高的等级，以引起相关人员的重视。

与资产赋值和威胁赋值一样，下面给出一个脆弱性严重程度赋值表，如表 9.2 所示。

表 9.2　脆弱性严重程度赋值

等　级	标　识	定　义
5	很高	如果被威胁利用，将对资产造成完全损害
4	高	如果被威胁利用，将对资产造成重大损害
3	中等	如果被威胁利用，将对资产造成一般损害
2	低	如果被威胁利用，将对资产造成较小损害
1	很低	如果被威胁利用，其对资产造成的损害可以忽略

读者可以将表 9.2 与本书 2.1.2 节有关系统定级的定义进行对比，从而加深对风险评估与等级保护相互关系的理解。

9.3　脆弱性识别案例分析

在本节中，将继续以“数字兰曦”为例，介绍如何进行脆弱性识别及该过程结束后怎样撰写技术报告。

实施脆弱性评估主要从技术和管理两个方面进行评估，涉及物理层、网络层、系统层、应用层、管理层等各个层面的安全问题。其中技术脆弱性评估主要是通过远程和本地两种方式进行系统扫描、对网络设备和主机等进行人工抽查方式进行的，以保证技术脆弱性评估的全面性和有效性；管理脆弱性评估则主要通过对兰曦公司提供的各种管理文档和人员访谈来进行。

在前期的《“数字兰曦”资产识别报告》中划分的 5 个主要业务子系统和 1 个网络平台的基础上，通过对各个子系统和网络平台的重要资产进行调查分析，对兰曦公司信息系统存在的脆弱性进行了详实分析。“数字兰曦”作为一个应用较为成熟的系统，经过多年的建设和实际应用的检验，系统各个方面的建设都较为完善。“数字兰曦”覆盖

了其管辖的 12 个分公司、1 个研究院和全国 145 个销售网点，系统外延广，纵深延伸深，系统复杂程度高，因此系统存在潜在脆弱性的可能性也较大。通过对系统的详细调研和分析，目前“数字兰曦”的脆弱性主要表现在以下 4 个方面。

1．网络脆弱性

例如，在“数字兰曦”系统中，结构安全与网段划分、网络访问控制、拨号访问控制、网络安全审计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备防护都涉及到，只是仍然存在一些考虑不周全的地方。例如，没有根据各部门的工作职能、重要性、所涉及信息的重要程度等因素，划分不同的子网或网段，没有对特定事件提供指定方式的实时报警，没有对网络设备的管理员登录地址进行限制等。

2．主机系统脆弱性

“数字兰曦”系统的身份鉴别、访问控制、系统保护、恶意代码防范方面都做得很好，唯一的不足就是在剩余信息保护。由于“数字兰曦”系统是按照第 3 级安全测评要求来建设的，所以风险评估中不涉及可信路径等方面的内容。

3．应用系统脆弱性

“数字兰曦”对身份鉴别、访问控制、剩余信息保护方面做了相应的工作，但在通信保密性、抗抵赖、软件容错、资源控制、代码安全等方面考虑得很少。

4．管理脆弱性

兰曦公司信息中心制定了相应的管理章程和制度来配合信息系统的运行，但在对相关人员进行定期安全业务培训方面存在问题，主要体现在 3 个方面：一是培训计划不完善，无论是年度培训计划时间安排、培训内容还是培训人员安排，均比较空泛；二是对以往的培训结果缺乏相应的总结和考核；三是缺乏演练性培训记录。此外，在制度执行的粒度上也存在问题。

9.3.1　信息环境脆弱性识别

1．软环境脆弱性识别——管理脆弱性

管理脆弱性又可分为**技术管理脆弱性**和**组织管理脆弱性**两个方面，并与管理环境相关。信息系统的管理脆弱性主要存在于管理制度资产、物理环境及保障设备资产、组织的安全和对安全事故及故障的响应方面。“数字兰曦”经过长期的运营维护，已有较为完善的规章管理制度，但各个规章制度的相互衔接和可操作性还有所欠缺。《中心机房管理办法》对进出机房的访问控制、机房环境的监控、机房内重要设备的访问控制进行了指导性的规定，但缺少更细粒度的操作规范说明；《“数字兰曦”网络安全管理办法》对公司内部工作人员使用、配置计算机和网络设备制定了统一的操作要求，但是缺少细粒度的技术要求（如密码设置的规则）和相应的监控管理办法；《兰曦公司关于加强行业互联网管理工作的通知》对本公司各部门接入互联网的办法进行了规定，但对已接入

互联网的部门缺少对互联网访问控制的具体管理规定。信息安全相关人员的教育培训只针对部分人员，同时未进行定期的培训。具体的管理脆弱性严重程度赋值如表 9.3 所示。

表 9.3　管理脆弱性严重程度赋值

序号	资产类别	资 产 名 称	脆弱性描述	严重程度等级	使用范围
1	管理资产	机房管理办法		1	“数字兰曦”
2	管理资产	信息安全策略文档		1	
3	管理资产	信息安全教育和培训	教育培训制定不规范	2	
4	管理资产	“数字兰曦”视频会议系统运行管理办法		1	
5	管理资产	“数字兰曦”建设及管理规范		1	
6	管理资产	“数字兰曦”网络安全管理办法	缺少细粒度的技术要求	2	
7	管理资产	中国电子工业集团关于加强行业互联网管理工作的通知		1	
8	管理资产	兰曦公司关于加强行业互联网管理工作的通知	缺少对互联网访问控制的具体管理规定	2	

2．软环境脆弱性识别——人员脆弱性

人员是信息系统安全的重要因素，因为信息系统的一切行为都是由人来实施和完成的，所以人员管理是信息安全管理的核心问题。人员脆弱性主要体现在对人员的管理方面。下面主要是针对人员的管理进行分析描述。

人员管理是对人员的安全和保密意识教育、安全技能培训情况，重点、敏感岗位人员有无特殊管理措施，对突发事件的责任，报告安全事故，脆弱点，用户培训等方面进行管理。人员管理主要通过单位或机构的组织的形式来体现，即单位或机构需要建立和完善其所属信息系统的信息安全的安全负责人和安全管理员组织体系。

在兰曦公司对人员的管理中，还存在着一些问题：① 对人员的再教育力度、制度不够明显、突出。对人员的再教育培训上，针对的是部分人员的再教育培训，这就会造成信息系统从业人员的专业素质参差不齐。在培训机制上，未进行定期的专业培训，这就造成人员无法了解最近的技术。② 尚未形成严格的人员考评机制。根据本单位人员的具体情况，将信息系统相关从业人员兰曦公司组织机构分成三类，根据每类人员的分析得出每类人员的脆弱性，如表 9.4 所示。

表 9.4　人员脆弱性严重程度赋值

序号	资 产 名 称	脆弱性名称	严重程度等级
1	公司信息化领导小组	人员脆弱性	2
2	公司信息中心	人员培训规范	2
3	分公司/研究院人员	人员培训不规范	3

3．硬环境脆弱性识别

机房是信息系统安全的重要基础设施，越来越受到人们的关注和重视。兰曦公司中

心机房是一个集各种路由器、网络交换机、机房网络物理基础设施等为一体的管理中心，引入了许多监控设施，正朝着智能化管理方向迈进。中心机房存放着“数字兰曦”的最核心设备，其建设标准达到了国家 A 级标准，对机房的投入比较大，期望通过正规化、科学化的机房建设，使信息系统各设备运行状况良好，并达到稳定、可靠和安全的要求。

根据国家机房建设标准的要求，机房管理要集中化，告警要人性化，对网络物理基础设施状况评估要快速化，对影响业务系统的事件要能够及时发觉，还需合理规划系统可用性、电源、运行时间及空调等需求。通过检查，发现“数字兰曦”中心机房仍存在着一些问题：机房内监控设备的覆盖率尚未达到 100%，存在监控死角。监控设备作为机房重要的防盗设备，是机房在物理安全上的一个重要保障，兰曦公司应该对机房监控设备进行完善，从而保证机房内的物理安全。

具体的中心机房脆弱性严重程度赋值如表 9.5 所示。

表 9.5　中心机房脆弱性严重程度赋值

序号	资 产 名 称	脆弱性名称	严重程度等级
1	机房位置与设备布置	机房管理脆弱性	1
2	环境条件	机房管理脆弱性	1
3	建筑	机房管理脆弱性	1
4	空气调节	机房管理脆弱性	1
5	电气技术	机房管理脆弱性	1
6	给水排水	机房管理脆弱性	1
7	消防安全	机房管理脆弱性	1
8	设备的管理还不够正规，还没有形成制度化	机房管理脆弱性	1
9	辅助安全措施还有缺陷	机房管理脆弱性	1
10	安全机制还不够完善	机房管理脆弱性	1
11	防盗监控	机房管理脆弱性	3
	……		

9.3.2　公用信息载体脆弱性识别

“数字兰曦”公用信息载体根据其载体功能划分为通信载体、安全防护载体、信息终端及存储设备。其中通信载体主要是指各个子系统进行通信、数据交换的所有交换机和路由器。安全防护载体指在通信中从一定程度上保证通信安全和保密的各种设备，主要是指网络防火墙、入侵检测设备、安全审计设备和漏洞扫描设备。信息终端指进行各种信息交互的设备，主要是指各种 PC、笔记本、打印机和扫描仪等。

通过对网络拓扑图的分析和各种设备的技术参数分析，“数字兰曦”公用信息载体脆弱性主要在网络的 VLAN 划分和部分设备上。

1．网络平台配置脆弱性

（1）“数字兰曦”子系统之间 VLAN 存在交叉划分问题，由“数字兰曦”网络拓扑图（见图 7.8）分析，各个子系统之间的服务器存在不同子系统服务划分在同一 VLAN 的情况。

该脆弱性带来的影响：根据此段漏洞扫描的结果，在此网段存在很容易让黑客利用的漏洞（具体请参考 9.3.3 节仿真实验报告）。如果攻击者利用一个漏洞成功控制此网段的任何一台服务器，就会对其他服务器造成非常大的威胁。特别是对“数字兰曦”非常重要的“兰芯”子系统，一旦服务器被直接或间接控制，会对整个信息系统产生非常严重的影响。

（2）与“兰芯”子系统联系非常紧密的办公自动化子系统服务器放在 DMZ 区。

该脆弱性带来的影响：这对“兰芯”子系统是非常危险的，因为 DMZ 区上的服务器都是外界能访问的。而此服务器同时能访问内网的其他服务器。这样，攻击者一旦攻破办公自动化子系统服务器，会对“兰芯”子系统造成非常严重的威胁。

2．公用信息载体脆弱性

在对“兰芯”子系统进行公用信息载体脆弱性识别的时候，其主要的脆弱性体现在以下交换设备中：

（1）CISCO 6506 trunk 端口由于其本身系统的原因，如果没有对其三层路由进行正确配置，不同 VLAN 之间可能不能正常传递，使得各种数据不能实现 VLAN 之间的共享和传递。

（2）CISCO 3550 由于其本身系统的原因不能实现 NAT 方式的网络地址转换，这样对地址域的映射会存在较大的影响。

（3）CISCO 7206 虽然支持网络地址转换（NAT），但是会增大系统处理的数据流量，使得其所支持的 NAT 状态不稳定。由此可能造成地址的映射不完整，对系统内各个通信客户端产生影响。

（4）CISCO 7206 路由器还存在需要重新启动后才能使用的硬件故障，其出现次数可能比较频繁，对正常网络通信会有较大的影响。

具体的公用信息载体脆弱性严重程度赋值如表 9.6 所示。

表 9.6　公用信息载体脆弱性严重程度赋值

序号	资 产 名 称	脆　弱　点	严重性等级
1	CISCO 6506	如果没有设定三层路由，VLAN 之间是不能相互访问的	3
2	CISCO 4506		1
3	CISCO 3550 系列	不能进行网络地址转换	2
4	s5126		1
5	QuidWay S6506R		1
6	QuidWay S3952P/S3928P		1

续表

序号	资 产 名 称	脆　弱　点	严重性等级
7	QuidWay S3928P		1
8	QuidWay NE20		1
9	CISCO　7206	服务器上数据流量很大，CISCO 7206 所支持的 NAT 就会很不稳定，可能出现不能使用，需要重新启动后才能使用的现象	3
10	CISCO 3745		1
11	CISCO 3825		1
12	QuidWay AR4640		1
13	CISCO 2600		1
14	互联网防火墙 4000V2		1
15	广域网防火墙 FortiGate 1000A		1
16	分公司防火墙 POWER-V 404		1
17	分公司防火墙 NETPOWER		1
18	“冰之眼”入侵检测 1600D		1
19	“天眼”入侵检测 NPIDS-100		1
20	主机入侵侦测 QuidWay S3928P		1
21	“极光”漏洞扫描“极光 V4”		1
			

3．专用信息及信息载体脆弱性识别——“兰芯”子系统

在“兰芯”子系统中，根据扫描的结果，可以得到威胁系统的相应脆弱点分别是 CVE-2004-0786、CVE-2004-0747、CVE-2004-0751、CVE-2004-0748、CVE-2004-0809、CVE-1999-0504、CVE-1999-0505 CVE-1999-0506、CVE-2000-0222、CVE-2002-1117 和 CVE-2005-3595。这些脆弱点又对不同的资产类产生不同的影响。这些脆弱点主要是针对 Windows 2003 和 HP Aix5.3 的漏洞进行攻击，主要表现为：

（1）信息欺骗漏洞（CVE-1999-0504、CVE-1999-0505、CVE-1999-0506、CVE-2000-0222、CVE-2002-1117、CVE-2005-3595）。由于操作系统的安装未对 guest 账户进行安全设置，攻击者可以利用空会话、guest 账户登录主机，并改变其系统的配置，造成严重后果。

该脆弱性带来的影响：信息欺骗漏洞出现在“兰芯”子系统的中心服务器操作系统中，该系统属于“数字兰曦”的核心系统，如果被攻击者通过 guest 账户等一些方式登录，就可以破坏系统的权限设置。

（2）拒绝服务漏洞（CVE-2004-0786、CVE-2004-0747、CVE-2004-0751、CVE-2004-0809）。HP 主机运行的 Apache 版本过于陈旧，低于 2.0.51 版本，是“兰芯”子系统的一个严重隐患。

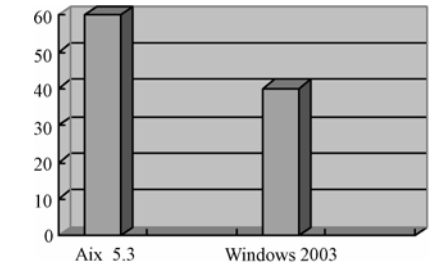


图 9.1　“兰芯”子系统主要漏洞统计图

该脆弱性带来的影响：拒绝服务漏洞一旦被攻击者利用，就可以停止系统中运行的 Apache 服务，而该系统又运行在“兰芯”子系统专用服务器上，一旦服务停止，系统将会受到严重的破坏，使用户无法访问。

以上两个主要的漏洞可以用图 9.1 形象地表现出来。

表 9.7 所示为对”兰芯”子系统专用信息及信息载体脆弱性的统计情况，由于本书篇幅所限，只罗列了部分脆弱性。

表 9.7　“兰芯”子系统专用信息及信息载体脆弱性统计情况

序号	资 产 类	资产名称	脆 弱 点	使用范围	备　注
1	计算机操作系统	Aix 5.3	CVE-2004-0786 CVE-2004-0747 CVE-2004-0751 CVE-2004-0748 CVE-2004-0809	“兰芯”专用服务器	IP:10.11.1.130 拒绝服务漏洞
2	计算机操作系统	Aix 5.3	CVE-2004-0786 CVE-2004-0747 CVE-2004-0751 CVE-2004-0748 CVE-2004-0809	“兰芯”专用服务器	IP:10.11.1.138 拒绝服务漏洞
3	计算机操作系统	Aix 5.3	CVE-2004-0786 CVE-2004-0747 CVE-2004-0751 CVE-2004-0748 CVE-2004-0809	“兰芯”数据库专用服务器	IP:10.11.7.150 拒绝服务漏洞
4	计算机操作系统	Windows 2000	CVE-1999-0504 CVE-1999-0505 CVE-1999-0506 CVE-2000-0222 CVE-2002-1117 CVE-2005-3595	研究院	IP:10.11.5.13 信息欺骗漏洞
5	计算机操作系统	Windows 2003	CVE-1999-0504 CVE-1999-0505 CVE-1999-0506 CVE-2000-0222 CVE-2002-1117 CVE-2005-3595	分公司	IP:10.11.6.126 信息欺骗漏洞
	……				

“兰芯”子系统专用信息及信息载体脆弱性严重程度赋值如表 9.8 所示。

表 9.8　专用信息及信息载体脆弱性严重程度赋值

序　号	资 产 名 称	脆弱性名称	严重程度等级
1	10.11.1.130　HP Aix5.3	拒绝服务漏洞	4
2	10.11.1.138　HP Aix5.3	拒绝服务漏洞	4
3	10.11.7.150　HP Aix5.3	拒绝服务漏洞	4
4	10.11.5.13　Windows 2000	信息欺骗漏洞	3
5	10.11.6.126　Windows 2003	信息欺骗漏洞	3
	……		

9.3.3　脆弱性仿真验证

在“专用信息及信息载体脆弱性识别”中已经罗列了“兰芯”子系统的许多 CVE 漏洞。下面通过仿真实验的方式向读者展示这些 CVE 漏洞一旦被成功利用会带来什么危害。

1.“兰芯”子系统“空口令”漏洞仿真实验

撰写实验报告是测评人员的基本功，因此我们先给出“兰芯”子系统中发现的“空口令”漏洞仿真实验的计划，如表 9.9 所示。

表 9.9　“空口令”漏洞仿真实验

实验名称	Windows 2000 Server 默认配置空口令
实验编号	略
CVE 编号	CVE-1999-0504、CVE-1999-0505
漏洞信息	默认配置空口令可使远程攻击者利用这一漏洞对服务器发起攻击
实验时间	略
实验地点	“深海”信息安全测评中心实验室
实验人员	“数字兰曦”项目组
备注	“数字兰曦”信息安全风险评估项目

1）实验案例描述

根据现场扫描的结果，IP 地址为 10.11.1.137 的服务器存在“空口令”漏洞，该服务器属于“兰芯”子系统，型号为 IBM X346 服务器，操作系统为 Windows 2000 Server。本实验针对 Windows 2000 Server 默认配置“空口令”的漏洞，搭建仿真平台，进行仿真渗透测试，以验证该漏洞被利用后对系统造成的影响。

2）仿真实验平台描述

用一台 PC 模拟存在“空口令”漏洞的服务器（即被攻击机，在“兰芯”子系统内为 IBM X346 服务器），安装 Windows 2000 Server 操作系统，并与实验小组的机器接在同一网段内，其 IP 地址设置为 192.168.1.71。另一台 PC（攻击机）安装 Windows XP 操作系统，其 IP 地址设置为 192.168.1.83。“空口令”仿真实验测试平台如图 9.2 所示。

3）仿真实验预期结果描述

“空口令”漏洞被成功利用后，攻击机（192.168.1.83）可以向被攻击机（192.168.1.71）发送任意数据。

4）仿真实验步骤

（1）使被攻击机系统设置为默认安装，口令设置为空，如图 9.3 所示。

（2）登录成功后可以看到本地磁盘（C:）下的当前文件，如图 9.4 所示。

（3）在攻击机（192.168.1.83）上打开命令窗口，测试能否与被攻击机（192.168.1.71）连通，测试结果如图 9.5 所示。

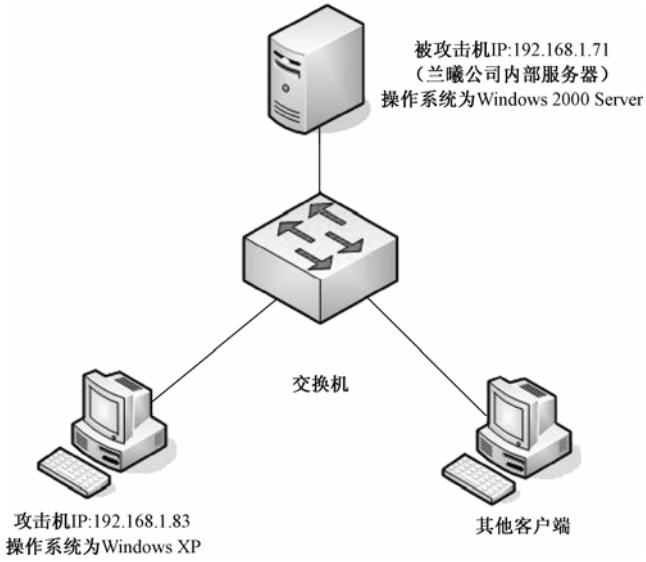


图 9.2　“空口令”仿真实验测试平台



图 9.3　被攻击主机的默认设置

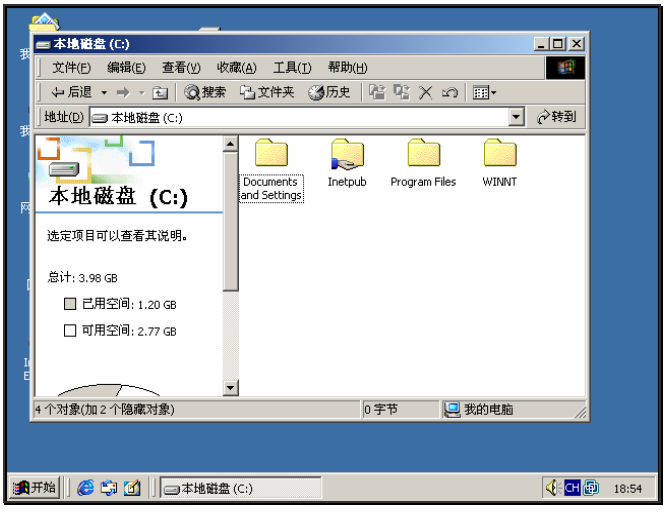


图 9.4　登录被攻击主机



图 9.5　从攻击机上 ping 被攻击主机

（4）在攻击机命令窗口下利用“net use”命令猜测被攻击机的口令，由于命令成功执行，说明远程主机可以通过“空口令”控制目标机，如图 9.6 所示。



图 9.6　猜测被攻击机登录口令

（5）攻击者可以向目标机发送一个木马程序，如图 9.7 所示。

（6）再打开目标机的 C 盘，可以看到攻击机已向被攻击机 C 盘上传了一个木马程序，如图 9.8 所示。

（7）这时攻击者可以进一步获得被攻击机上的时间信息，并设定一个时间值让这个文件自动执行。

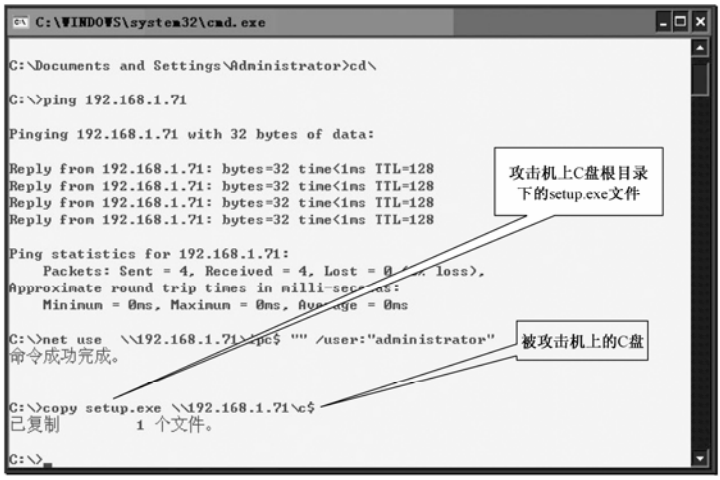


图 9.7　从攻击机上传木马程序至被攻击机



图 9.8　被攻击机上的木马程序

5）攻击行为特征描述

上述攻击属于利用被攻击机系统默认口令的漏洞，攻击者可以先利用“空口令”方式进行试探，如果不成功再进行口令猜测。

6）仿真实验总结

通过仿真测试，说明 Windows 2000 Server 的“空口令”设置是一个很容易被攻击者利用的漏洞。由于存在该漏洞的服务器所在子系统是整个“数字兰曦”中较为重要的系统，因此该漏洞一旦被成功利用，将对“兰芯”子系统造成严重影响，甚至可能威胁整个信息系统的安全。

2．Apache Tomcat 目录和文件暴露漏洞的仿真验证

Apache Tomcat 仿真实验计划如表 9.10 所示。

表 9.10　Apache Tomcat 仿真实验计划

实验名称	Apache Tomcat 目录和文件暴露漏洞
实验编号	略
CVE 编号	CVE-2003-0042
漏洞信息	安装 Apache Tomcat 3.3.1 及之前的版本，当其使用的 JDK 是 1.3.1 及之前的版本时，可允许远端攻击者获得敏感信息。如果远端攻击者发出 URL 请求，并加上空位元的字元（如 GET /.jsp HTTP/1.0），服务器将回应目录列表给攻击者
实验时间	略
实验地点	“深海”信息安全测评中心实验室
实验人员	“数字兰曦”项目组
备注	“数字兰曦”信息安全风险评估项目

1）仿真实验案例描述

根据现场扫描的结果，可知 IP 地址为 10.11.1.137 的服务器存在 Apache Tomcat 目录和文件暴露漏洞，该服务器属于“兰芯”子系统，型号为 IBM X346 服务器，操作系统为 Windows 2000 Server。本实验针对 Apache Tomcat 目录和文件暴露漏洞，搭建仿真平台，进行仿真渗透测试，以验证该漏洞被利用后对系统造成的影响。

2）实验平台描述

用一台 PC 模拟存在漏洞的服务器（即被攻击机，在兰曦公司内网为 IBM X346 服务器），安装 Windows 2003 Enterprise Server 操作系统，并与实验小组的机器接在同一网段内，其 IP 地址设置为 192.168.1.94。另一台 PC（攻击机）安装 RedHat Linux 9 操作系统，其 IP 地址设置为 192.168.1.98。Apache Tomcat 仿真实验测试平台如图 9.9 所示。

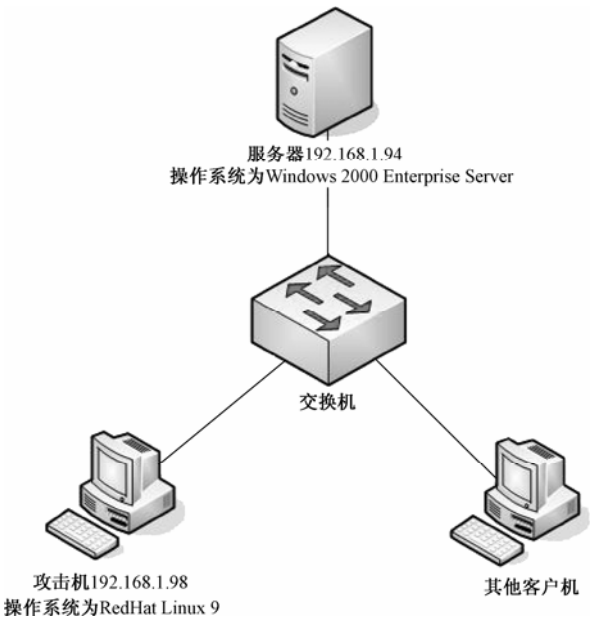


图 9.9　Apache Tomcat 仿真实验测试平台

3）仿真实验预期结果描述

当 Apache Tomcat 目录和文件暴露漏洞被成功利用后，被攻击机对外提供的 Web 服务将被阻断。

4）仿真实验步骤

（1）安装 jdk，版本号为 1.3，如图 9.10 所示。



图 9.10　安装 jdk

（2）配置 jdk 的环境变量，加入 JAVA_HOME　PATH 环境变量，如图 9.11 所示。

（3）修改注册表，对 jdk 进行修改。把“Jave 运行时的环境”改为“Java Runtime Environment”，如图 9.12 所示。



图 9.11　配置 jdk

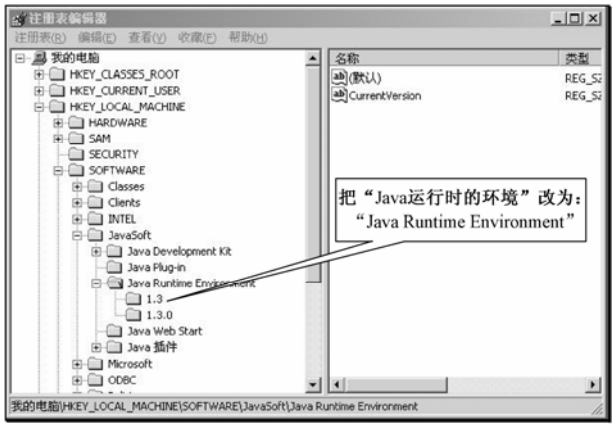


图 9.12　修改 jdk 注册表

（4）安装 Tomcat，对 Tomcat 的压缩文件进行解压，并放到目录 C:\下。

（5）测试Tomcat的连通性：输入 http://192.168.1.94:8080，如果显示图 9.13 所示的界面，那么可以推断Apache Tomcat服务器运行正常。

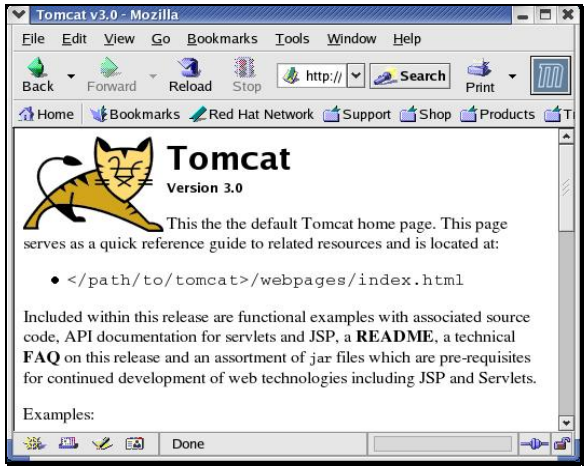


图 9.13　Tomcat 连通性检查

之后，利用此漏洞的 perl 语言工具进行漏洞攻击，如图 9.14 所示。

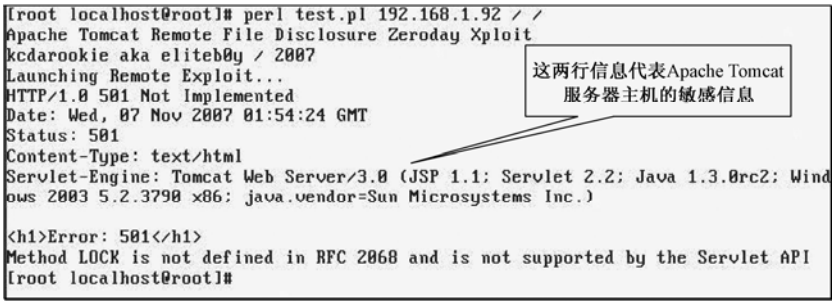


图 9.14　获取目标的敏感信息

5）攻击行为特征描述

上述攻击属于利用目标机系统 Apache Tomcat 服务器目录和文件暴露的漏洞，获得对方 Apache Tomcat 主机的敏感信息。

6）实验总结

通过仿真测试，说明 Apache Tomcat 服务器目录和文件暴露漏洞是一个很容易被攻击者利用的漏洞。由于存在该漏洞的服务器所在子系统是整个“数字兰曦”中较为重要的系统，因此该漏洞一旦被成功利用，将对“兰芯”子系统造成严重影响，甚至可能威胁整个信息系统的安全。图 9.15 表明我们利用这个漏洞进行的操作结果。

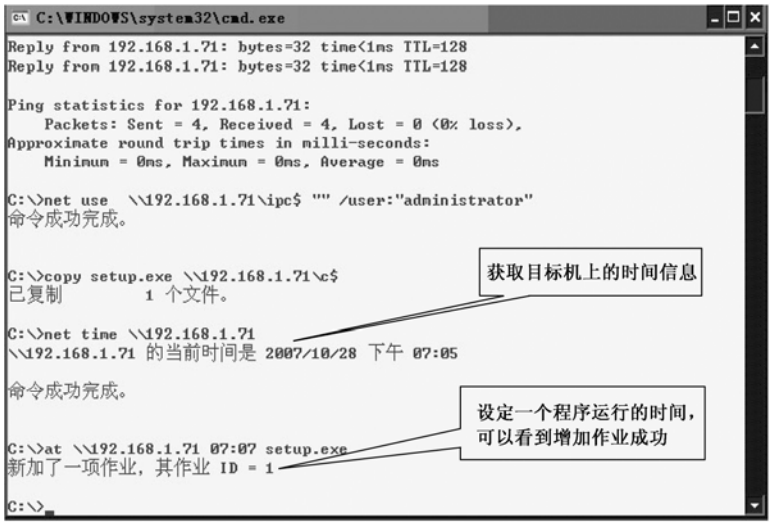


图 9.15　漏洞利用结果

3．大模块编码HTTP所造成的阻断服务仿真实验

大模块编码 HTTP 仿真实验计划如表 9.11 所示。

表 9.11　大模块编码 HTTP 仿真实验计划

实验名称	大模块编码 HTTP 引起的阻断服务攻击漏洞
实验编号	略
CVE 编号	CVE-2002-0392
漏洞信息	Apache 在处理某种大模块的编码 HTTP 要求时，Apache v1.3 到 v1.3.24 会允许远端攻击者执行任意程序（UNIX 系统），而 Apache v2.0 到 v2.0.36 会造成阻断服务
实验时间	略
实验地点	“深海”信息安全测评中心实验室
实验人员	“数字兰曦”项目组
备注	“数字兰曦”信息安全风险评估项目

1）仿真实验案例描述

根据现场扫描的结果，确定 IP 地址为 10.11.1.137 的服务器存在大模块编码 HTTP

引起的阻断服务攻击漏洞，该服务器属于“兰芯”子系统，型号为 IBM X346 服务器，操作系统为 Windows 2000 Server。本实验针对 Apache 大模块编码 HTTP 引起的阻断服务攻击漏洞，搭建仿真平台，进行仿真渗透测试，以验证该漏洞被利用后对系统造成的影响。

2）实验平台描述

用一台 PC 模拟存在漏洞的服务器（即被攻击机，在兰曦公司内为 IBM X346 服务器），安装 Windows 2000 Enterprise Server 操作系统，并与实验小组的机器接在同一网段内，其 IP 地址设置为 192.168.1.92。另一台 PC（攻击机）安装 RedHat Linux 7.3 操作系统，其 IP 地址设置为 192.168.1.80。大模块编码 HTTP 仿真测试平台如图 9.16 所示。

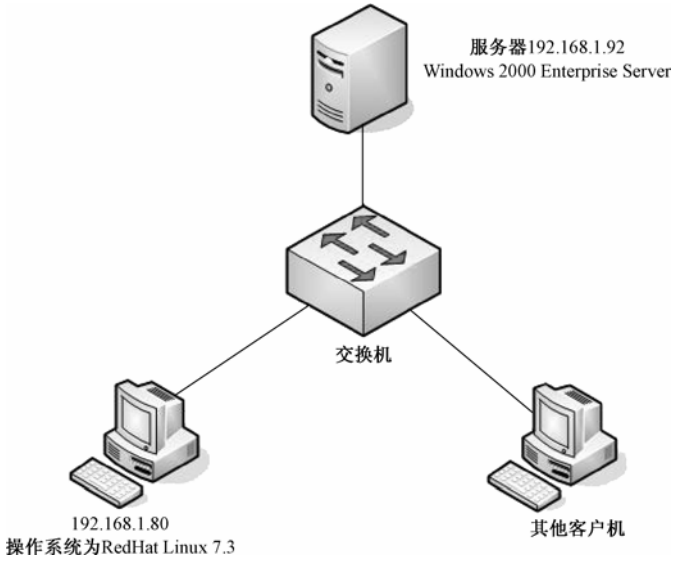


图 9.16　大模块编码 HTTP 仿真测试平台

3）仿真实验预期结果描述

大模块编码 HTTP 所造成的阻断服务攻击漏洞被成功利用后，被攻击机对外提供的 Web 服务将被阻断。

4）仿真实验步骤

（1）安装版本为 1.3.22 的 Apache。

（2）在 Microsoft Visual C++上对攻击程序 Apache-Slasher.c 进行编译，生成 Apache-Slasher 可执行程序。

（3）关闭防火墙。

（4）在攻击机（192.168.1.80）上打开命令窗口，测试能否与被攻击机（192.168.1.92）连通，测试结果如图 9.17 所示。

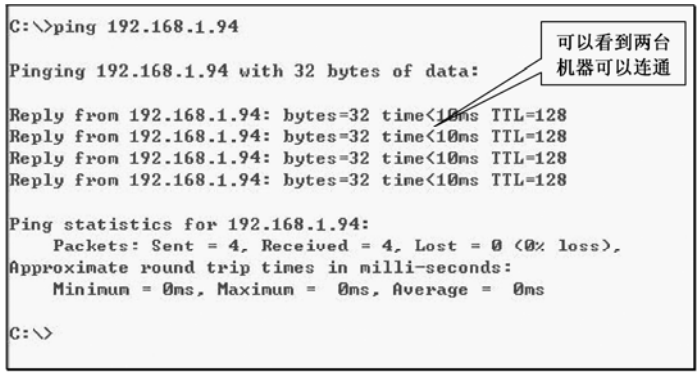


图 9.17　从攻击机端 ping 被攻击机

（5）利用 HTTP 大模块阻断服务攻击工具 Apache-Slasher 来攻击 Windows 2000 Enterprise Server 中的 Apache 服务器，如图 9.18 所示。



图 9.18　启动攻击工具

（6）攻击程序发送大模块 HTTP 编码的过程，如图 9.19 所示。

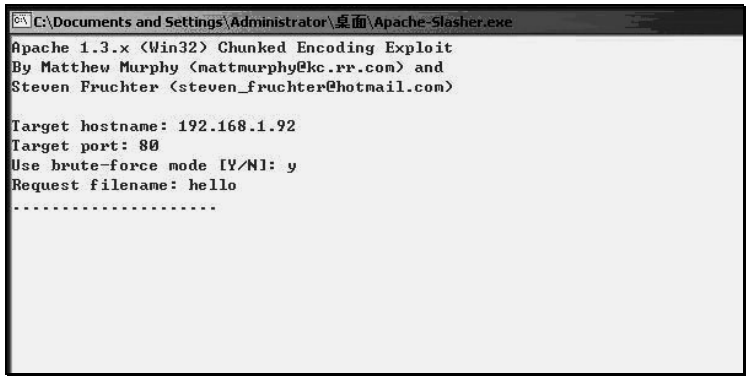


图 9.19　开始攻击

（7）被攻击主机的内存遭到大量占用，使响应时间变得迟缓，如图 9.20 所示。

5）攻击行为特征描述

上述攻击属于利用目标机系统 Apache 服务器大模块编码 HTTP 引起的阻断服务攻击漏洞，攻击者可以利用该漏洞阻断对方的 HTTP 请求。

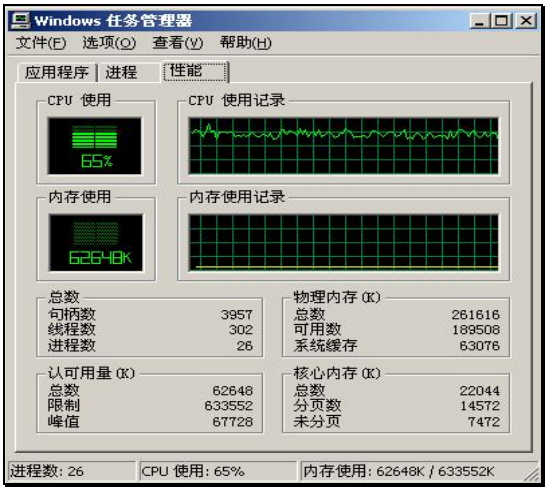


图 9.20　被攻击机资源逐渐耗尽

6）仿真实验总结

通过仿真测试，说明 Windows 2000 Enterprise Server Apache 的大模块编码 HTTP 引起的阻断服务攻击漏洞，是一个很容易被攻击者利用的漏洞。由于存在该漏洞的服务器所在子系统是整个“数字兰曦”中较为重要的系统，因此该漏洞一旦被成功利用，将对“兰芯”子系统造成严重影响，甚至可能威胁整个信息系统的安全。

4．mod_rewrite模块缓冲区溢出漏洞仿真实验

mod_rewrite 模块缓冲区溢出漏洞仿真实验计划如表 9.12 所示。

表 9.12　mod_rewrite 模块缓冲区溢出漏洞仿真实验计划

实验名称	mod_rewrite 模块缓冲区溢出漏洞
实验编号	略
CVE 编号	CVE-2003-0542
漏洞信息	Apache HTTP Server 1.3.29 及 2.0.48 之前版本的 mod_rewrite 模块存在缓冲区溢出漏洞，攻击者可以通过创建特制的配置文件导致拒绝服务或执行任意程序
实验时间	略
实验地点	“深海”信息安全测评中心实验室
实验人员	“数字兰曦”项目组
备注	“数字兰曦”信息安全风险评估项目

1）仿真实验案例描述

根据现场扫描的结果，确认 IP 地址为 10.11.1.137 的服务器存在 mod_rewrite 模块缓冲区溢出漏洞，该服务器属于“兰芯”子系统，型号为 HP，操作系统为 Windows 2003 Enterprise Server。本实验针对 Apache 的 mod_rewrite 模块缓冲区溢出漏洞实验，搭建仿真平台，进行仿真渗透测试，以验证该漏洞被利用后对系统造成的影响。

2）仿真实验平台描述

用一台 PC 模拟存在漏洞的服务器（即被攻击机，在兰曦公司内为 IBM X346 服务器），安装 Windows 2003 Enterprise Server 操作系统，并与实验小组的机器接在同一网段内，其 IP 地址设置为 192.168.1.94。另一台 PC（攻击机）安装 RedHat Linux 9 操作系统，其 IP 地址设置为 192.168.1.98。mod_rewrite 仿真测试平台如图 9.21 所示。

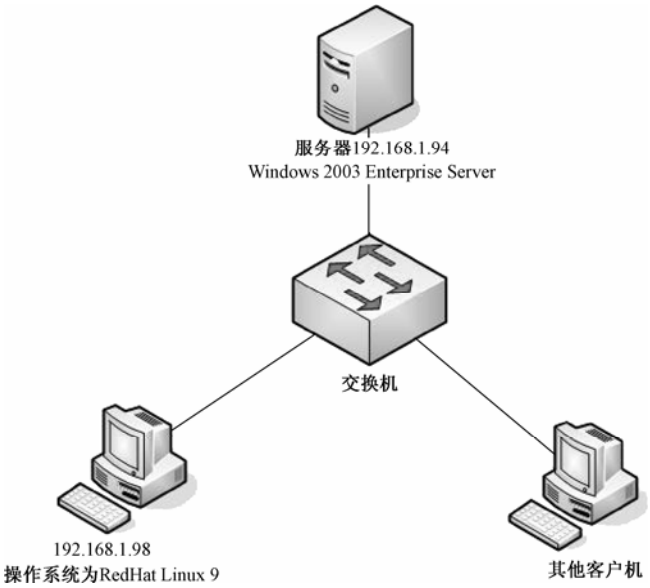


图 9.21　mod_rewrite 仿真测试平台

3）仿真实验预期结果描述

mod_rewrite 模块缓冲区溢出漏洞被成功利用后，被攻击机向攻击机反馈一个 shell 命令行。

4）仿真实验步骤

（1）安装版本号为 2.0.58 的 Apache 服务器软件。

（2）对 Apache 程序的配置文件进行修改，分别如图 9.22、图 9.23 和图 9.24 所示。

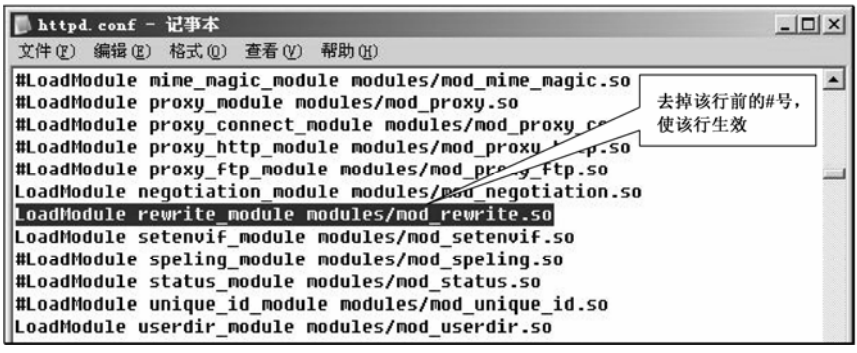


图 9.22　修改 Apache 配置文件（1）

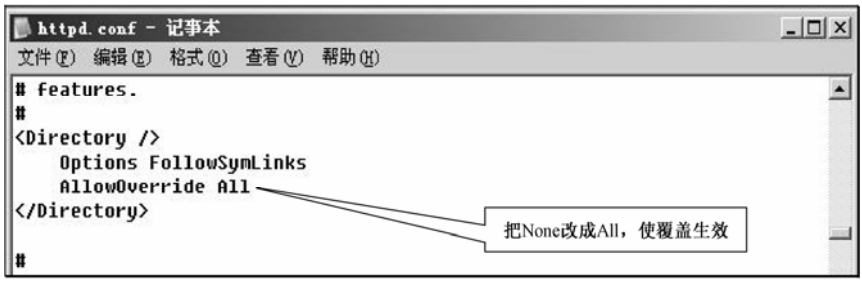


图 9.23　修改 Apache 配置文件（2）

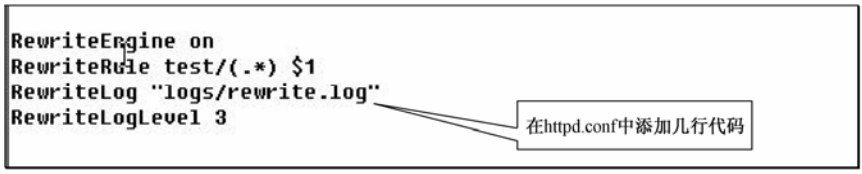


图 9.24　修改 Apache 配置文件（3）

（3）对攻击程序 exploit.c 进行编译，生成 exploit 可执行程序，如图 9.25 所示。



图 9.25　生成可执行的攻击程序

（4）使用命令行指令“iptables -F”关闭防火墙，如图 9.26 所示。

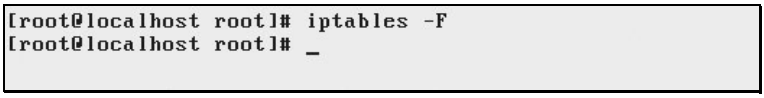


图 9.26　关闭被攻击机防火墙

（5）在攻击机（192.168.1.98）上打开命令窗口，测试能否与被攻击机（192.168.1.94）连通，测试结果如图 9.27 所示。

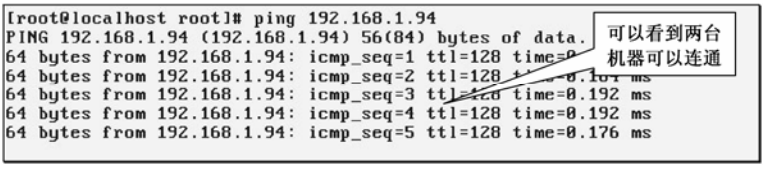


图 9.27　从攻击机端连接被攻击机

（6）利用 mod_rewrite 模块缓冲区溢出漏洞攻击工具 exploit 来攻击 Windows 2003 Enterprise 中的 Apache 服务器 mod_rewrite 模块，如图 9.28 所示。

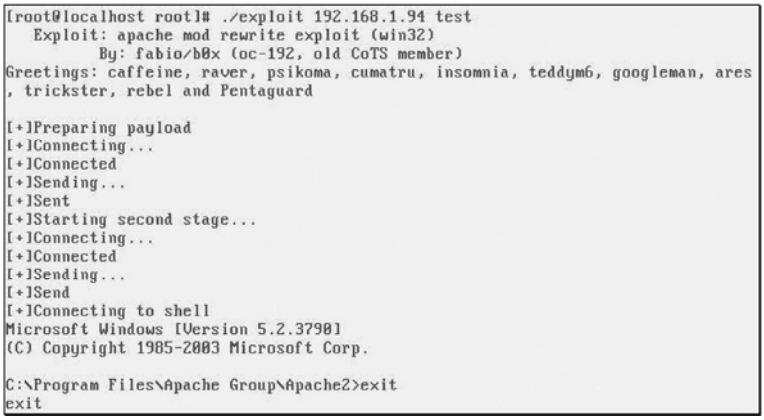


图 9.28　对 mod_rewrite 模块进行攻击

（7）攻击者可以任意删除程序（如删除 README.txt），如图 9.29 所示。

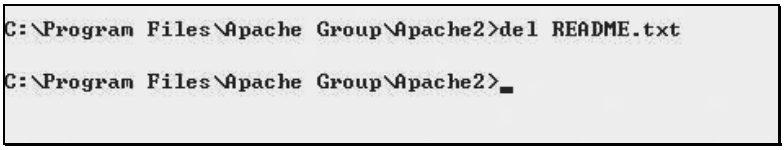


图 9.29　攻击成功后可继续进行破坏

5）攻击行为特征描述

上述攻击属于利用目标机系统 Apache 服务器 mod_rewrite 模块缓冲区的溢出漏洞，得到对方的 shell 命令行。

6）仿真实验总结

通过仿真测试，说明 Windows 2003 Enterprise Server Apache 的 mod_rewrite 模块缓冲区溢出漏洞攻击，是一个很容易被攻击者利用的漏洞。由于存在该漏洞的服务器所在子系统是整个“数字兰曦”中较为重要的系统，因此该漏洞一旦被成功利用，将对“兰芯”子系统造成严重影响，甚至可能威胁整个信息系统的安全。

9.3.4　脆弱性识别输出报告

本章结束之际，也需要输出一个技术报告——《脆弱性识别报告》。报告的主体包括被评估单位系统脆弱性的分类和脆弱性赋值等。以本章案例为例，该报告的格式如下所示。

错误！

“深海”信息安全测评中心

“数字兰曦”脆弱性识别报告

摘要
目录
图标目录
报告审批（授权签字）及日期
1　撰写依据
2　术语解释
3　脆弱性赋值原则和方法
4　“数字兰曦”系统脆弱性概述
5　“数字兰曦”脆弱性分类与赋值
5.1　“兰芯”子系统脆弱性分类与赋值
5.2　“兰剑”子系统脆弱性分类与赋值
5.3　……
6　附录

9.4　本章小结

- 脆弱性识别的出发点和立足点
- 脆弱性的概念
- 脆弱性识别的概念
- 脆弱性的验证
- 脆弱性赋值要综合考虑的因素
- 脆弱性识别报告

尾声：木马歌

古希腊诗人荷马在其史诗伊利亚特与奥德赛里记载了著名的特洛伊（Trojan）战争。关于特洛伊战争，有一个故事叫做《木马屠城记》，据荷马史诗和希腊神话，事起一个女人。

主神宙斯（Zeus）当年本与忒提斯（Thetis）相恋，但传说忒提斯之子将比其父更强，所以宙斯担心他本人当年推翻父亲的事重演，于是将忒提斯嫁给了著名英雄珀琉斯（Peleus）。

在忒提斯与佩琉斯的婚礼上，邀请了所有的神，但争吵女神却未受邀请。一气之下，争吵女神抛出一个金苹果，上写“给最美丽者”。三个女神雅典娜、阿佛洛狄德和希拉都宣称自己应该获得这个苹果。最后她们请求特洛伊王子帕里斯裁决。为得到金苹果，三个

女神争相贿赂帕里斯：雅典娜以天下第一聪明人作贿赂；阿佛洛狄德以天下第一美人作贿赂；希拉以王位作贿赂。最后帕里斯选择了阿佛洛狄德。于是，帕里斯与斯巴达王后——世上最美女人海伦相爱了，并在一次访问斯巴达时抢走了海伦，带她到了特洛伊。

斯巴达国王内劳斯因王后被抢走而恼羞成怒，便向希腊各城邦求助，联合向特洛伊宣战。

特洛伊有亚马逊女战士和黎明女神的儿子梅农的帮忙，又有维纳斯的暗中协助，有力地抵抗了希腊联军。但是，雅典娜因没得到金苹果，一直怀恨在心，这时便指示奥德修斯向希腊联军献上了后来著名的木马屠城之计。一天，希腊联军突然撤退，并留下一只木马（后来被称为特洛伊木马，Trojan Horse），特洛伊人将其当作战利品带回城内。当夜，当特洛伊士兵为胜利而庆祝时，藏匿在木马中的希腊士兵钻出木马，悄悄打开城门，迎进城外的希腊联军，这样一个里应外合，在一夜间就将特洛伊城内的所有男人斩尽杀绝。

木马屠城记的故事过去长期被世人看作是希腊神话，没有被认为是真实的。但是到了 19 世纪，业余考古学者苏利曼却证实了木马屠城记其实确有其事。

无数的史实不断地警示世人，当我们在全力抵御来自外面的敌人时，别忘了从内部严加防范。请君听我“木马歌”：

金城汤池不可进
铜墙铁壁不可攻
千古传奇木马计
堡垒最易从内破

观感

（1）脆弱性赋值和资产赋值的关系是什么？

（2）为什么脆弱性识别过程中需要进行脆弱性验证？

（3）请在网上下载 Nessus 和 X-Scan 等扫描软件并对自己的计算机进行脆弱性扫描。试比较二者之间的异同。

（4）请在国家权威信息安全测评机构，如中国国家信息安全产品测评中心网站上检索有哪些国产扫描工具通过了国家测评机构的检测。

（5）在权威安全机构网站上查询网络设备的 CVE 信息，如 CISCO FWSM 模块的脆弱性信息。

（6）请在本章案例分析的基础上完成《“兰芯”子系统脆弱性识别报告》。

（7）试分析“杜甫”子系统（见本书第 3 章最后“观感”）的脆弱性，并按照本章给出的脆弱性识别报告模式撰写《“杜甫”子系统脆弱性识别报告》（您可能需要第 7、8 两章“观感”部分的资产识别和威胁识别报告）。

第 10 章

风 险 分 析





长城烽火图

烽火照西京，心中自不平。
牙璋辞凤阙，铁骑绕龙城。
雪暗凋旗画，风多杂鼓声。
宁为百夫长，胜作一书生。

——杨炯 《从军行》

序幕：烽火的演变

在人类文明的历史长河中，截止到无线电发明之前，人们对战争威胁的预警方式可谓“八仙过海，各显神通”。如果按照预警速度来比较，大致可以分为这样几类：利用人工预警，如第一位马拉松金牌获得者雅典士兵裴里匹底斯，速度为 20 km/h 左右；利用动物预警，如西夏王国军队的信鸽，速度为 80 km/h 左右；利用音速预警，如公元前 6 世纪北欧斯堪第纳维亚人的号角和非洲部落的战鼓；利用光速预警，如公元前 8 世纪中国就开始使用的烽火。

“烽火戏诸侯”固然说明了周幽王的昏庸与腐败，但从另外一个角度也证明了古代中国的联军纪律严明、准备充分、反应迅速。

到了公元 8 世纪，大唐帝国国防部（兵部）在总结过去一千多年烽火预警方式的基础上，颁布实施了世界上最早的战略防御系统——长城烽火台。使用烽火的国家标准（《烽式》（唐））为：一炬为平安无事，二炬、三炬、四炬依次代表入侵敌军的规模大小。

现代社会，人们分别用蓝色、橙色、黄色、红色来预报各种自然灾害的严重程度，军队则用三级战备、二级战备、一级战备来代表战争威胁的不断加大。那么，信息安全风险呢？

要点：本章结束之后，读者应当了解和掌握

- 什么是风险分析？
- 什么是风险等级？
- 如何计算风险等级？
- 什么是风险控制？

- 怎样进行风险控制？
- 风险评估要提交哪些报告或清单？

10.1　风险分析概述

现在可以站在资产识别、威胁识别和脆弱性识别的基础上，对风险分析做一个整体的交代了。首先给出风险分析的定义。



风险分析（risk analysis），指依据国家有关标准对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行分析和评价的过程。它要分析资产面临的威胁及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

下面有 2 个相关的概念简要说明一下。

1．风险分析和风险评估



在信息安全领域（其实不仅仅是这个领域），风险分析与风险评估（risk assessment）是两个等同的概念，经常可以互换使用。如果要说两者之间有什么“细微”的差异的话，那就是风险分析更学术化一点，如可能会给人一种更偏重分析方法研究的感觉；风险评估更工程化一点，强调整个评估过程的规范性和程序正确性。但在本文中无意从这个角度来区分。作者在这里采用“风险分析”作为这一章的名称仅仅是因为避免与本书书名重复，特此说明。

2．风险分析和风险管理

风险分析（评估）与风险管理（risk management）就不是一对同义语了。风险管理包括了风险分析（评估）。而且两者从各自遵循的国家/国际标准来讲也是不一样的。我们将在本书最后一章对风险管理做一个简介。

那么风险分析与前面所介绍的资产识别、威胁识别和脆弱性识别的关系是什么呢？答案是风险分析将在这个基础上进行风险计算，对风险进行定级，提出相应的风险控制措施（也就是安全解决方案），最后再次评估残余风险，从而使得人们对信息系统所面临的风险从模糊的感觉上升到更为科学、理性的认识上面来。下面分别介绍风险计算、风险定级、风险控制和残余风险等相关内容。

10.2　风险计算

资产、威胁和脆弱性是风险的 3 个基本要素。在完成了资产识别、威胁识别和脆弱性识别之后，将采用适当的计算方法来确定威胁利用脆弱性导致安全事件发生的可能

性，并且根据资产价值及脆弱性的严重程度，最终判断安全事件一旦发生之后对组织造成的影响。这个影响值称为“**风险值**”。风险值计算关系如图 10.1 所示。

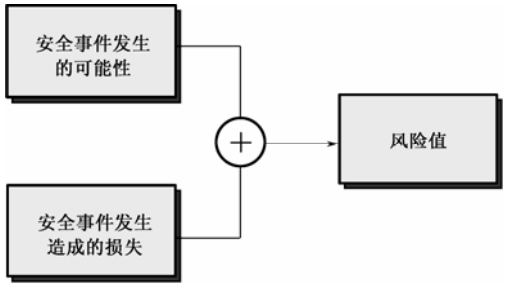


图 10.1　风险值计算关系图

风险值计算的形式化表示方法为

$$\text{风险值} = R(A,T,V) = R\left(L\left(T,V\right),F\left(I_{\text{a}},V_{\text{a}}\right)\right)$$

在第一个等式中，R 表示风险计算函数，A（Asset）表示资产，T（Threat）表示威胁，V（Vulnerability）表示脆弱性。这个等式表明风险值是由资产值、威胁值和脆弱性值这 3 个基本值综合确定的。当然，这仅是对风险值的一个定性的“数学模型”。如果仅停留在这一步，那么我们对风险的认识依然是原始的、模糊的，因为人们已经知道风险与资产、威胁和脆弱性相关。

为了计算 R，在实际工作中采用的是风险值的第二个计算公式。式中，I_{a} 表示安全事件所施加的资产的价值，V_{a} 表示这个资产的脆弱性严重程度，函数 L 表示威胁利用资产脆弱性的可能性，函数 F 表示一旦被成功利用之后所造成的损失。风险值的计算需要经过以下 3 个步骤。

1．计算安全事件发生的可能性 $L\left(T,V\right)$

根据威胁出现频率及脆弱性的状况，计算威胁利用脆弱性导致安全事件发生的可能性，即

$$\text{安全事件的可能性}=L\text{（威胁出现频率，脆弱性）}= L\left(T,V\right)$$

从理论上来讲，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（包括技术上和管理上的难易程度）和资产吸引力等因素来判断安全事件发生的可能性。但正如本书 8.2.1 节所述，要确定“虚拟空间中”的攻击者的技术能力是不太现实的，因为在 Internet 高度发达的今天，攻击技术的分享也呈现出全球化的趋势。所以读者在计算安全事件发生的可能性的时候，更多的要考虑从历史数据（或日志分析）中凝练出来的威胁出现频率 T 和资产脆弱值 V 这两个因素。

2．计算安全事件发生后的损失 $F\left(I_{\text{a}},V_{\text{a}}\right)$

根据资产价值及脆弱性严重程度，计算安全事件一旦发生后造成的损失，即

$$\text{安全事件造成的损失}=F\text{（资产价值，脆弱性严重程度）}= F\left(I_{\text{a}},V_{\text{a}}\right)$$

有时候安全事件的发生造成的损失不仅是针对资产本身，还可能影响业务的连续性，如金融机构核心数据被破坏，不仅是数据资产的损失，还将直接影响金融业务的正常运行，这就好比地震本身造成的损失有时候还不及次生灾害带来的负面影响一样。

3．计算风险值*R*

根据计算出来的安全事件的可能性及安全事件造成的损失，计算风险值，即

$$\text{风险值}=R(\text{安全事件的可能性，安全事件造成的损失})$$
$$=R(A,T,V)=R\left(L(T,V),F\left(I_{\mathrm{a}},V_{\mathrm{a}}\right)\right)$$

这里需要向读者指出两点：一是计算结果的相对性，即计算出来的风险值 R（往往是一个整数）是一个相对的概念。换言之，一个信息系统有若干子系统，这些子系统的风险值大小的比较是相对的。二是计算方法的相对性。目前，国内外风险值计算方法有很多，但无论哪种方法，最后都应该有归一性，即不同的计算方法对同一对象风险值的计算应该是相对一致的，不能出现采用 A 算法对信息系统 S 的风险值得出的结果，与采用 B 算法得出的结果大相径庭的情景。

下面向读者介绍一种常用的风险值算法——“相乘法”。我们将使用相乘法来分别计算安全事件发生的可能性 $L(T,V)$、安全事件造成的损失 $F(I_{\mathrm{a}},V_{\mathrm{a}})$和综合两者之后的风险值 R。评估者可根据自身情况选择其他的风险计算方法。相乘法适用于由两个或两个以上要素值确定一个要素值的情形。在上面计算风险值的 3 个步骤中，函数 L、F 及最终的 R 均是二元函数，所以我们将利用相乘法来计算风险值。相乘法是一种定量的计算方法，直接利用两个（或两个以上）要素值进行相乘得到另一个要素值，简单、自然，且可操作性强，因此在风险计算中应用较为普遍。相乘法原理和步骤如下介绍。

10.2.1　相乘法原理

设二元函数

$$z=f(x,y)=x\otimes y$$

式中，算子（即运算方式）可以事先加以定义，如对安全事件发生可能性最自然的理解就是

$$\text{安全事件可能性}=\text{威胁发生频率}\times\text{脆弱性严重程度}$$

所以可以直接定义

$$z=f(x,y)=x\otimes y=x\times y$$

但在实际工作中，如果上述直接相乘获得的值“跳跃性”较大（所有安全事件可能性的值计算完之后，其值域从 1～10 000），也常常对这些值进行“柔化”处理，使其符合我们的常识，也有利于最后进行风险等级的划分。常见的柔化处理方式包括

$$z=f(x,y)=x\otimes y=\left\lfloor\sqrt{x\times y}\right\rfloor$$

$$z = f(x,y) = x \otimes y = \left\lceil \frac{\sqrt{x \times y}}{x + y} \right\rceil$$

式中，⌊ ⌋和⌈ ⌉分别表示取（整数）下界和上界。

下面通过一个相乘法计算示例使读者熟悉风险计算的 3 个环节。

10.2.2　风险值计算示例

假设某资产的重要性赋值是 $A_1 = 5$，它面临两个威胁，其威胁发生频率值分别为 $T_1 = 25$ 和 $T_2 = 17$；T_1 可以利用 A_1 存在的两个脆弱性，其赋值分别是 $V_1 = 2$ 和 $V_2 = 3$；T_2 可以利用 A_1 存在的另外三个脆弱性，其赋值分别为 $V_3 = 1$、$V_4 = 4$ 和 $V_5 = 2$，因此资产 A_1 面临的风险值一共有 5 个。这 5 个风险值的计算方法完全一样，现在以 A_1 面临的威胁发生频率值 T_1 及 T_1 可以利用的脆弱性赋值 V_1 为例，来计算 A_1 面临的风险值。我们将采用公式

$$z = f(x,y) = x \otimes y = \left\lfloor \sqrt{x \times y} \right\rfloor$$

（1）安全事件发生的可能性 $L(T,V)$

$$z = f(x,y) = L(T,V) = \left\lfloor \sqrt{T_1 \times V_1} \right\rfloor = \left\lfloor \sqrt{25 \times 2} \right\rfloor = 7$$

（2）计算安全事件造成的损失 $F(I_a,V_a)$

$$z = f(x,y) = F(I_a,V_a) = \left\lfloor \sqrt{A_1 \times V_1} \right\rfloor = \left\lfloor \sqrt{5 \times 2} \right\rfloor = 3$$

（3）计算风险值 R

$$R = R(A,T,V) = R\left(L(T,V), F(I_a,V_a)\right) = \left\lfloor \sqrt{7 \times 3} \right\rfloor = 4$$

同理可以计算 A_1 的其他 4 个风险值。

10.3　风险定级

众所周知，地震的破坏性（地震烈度）分为多种等级，地震烈度可分为从 1 度直到 12 度，对应于不同的地震烈度，有“破坏性地震”、“毁灭性地震”和“歼灭性地震”等，其中烈度为 10～11 度之间的地震称为“毁灭性地震”（如这次汶川大地震），12 度以上就称为“歼灭性地震”。

为实现对风险的有效控制，可以像前面对资产、威胁和脆弱性那样，对风险评估的结果进行等级化处理。风险可划分为 5 个等级，等级越高，风险越高。

评估者应根据所采用的计算方法（如相乘法），计算每种资产面临的风险值，根据自身工程经验、被评估单位的实际情况和风险值的分布状况，为每个风险等级设定风险值范围，并对所有风险计算结果进行等级化处理。每个风险等级代表了相应风险的严重

程度，如表 10.1 所示。

表 10.1　风险等级划分

等级	标识	描　　述
5	很高	一旦发生将产生非常严重的经济或社会影响，如严重破坏组织信誉、严重影响组织的正常经营，经济损失重大、社会影响恶劣
4	高	一旦发生会产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面不大，影响程度不深
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补

我们再次建议读者将表 10.1 与本书 2.1.2 节有关系统定级的定义进行对比思考。

在 10.2.2 节风险值计算示例中，已经得到了 A_1 的一个风险值，最后需要确定威胁发生频率值 T_1 及 T_1 可以利用的脆弱性赋值 V_1 给 A_1 带来的风险等级。这时需要根据自身的工程经验和被评估单位的实际情况先制定一个风险值与风险等级的对照表，如表 10.2 所示。

表 10.2　风险等级划分示例

风险值	1～3	4～10	11～13	14～19	20 以上
风险等级	1	2	3	4	5

从这个对照表，可以查出 10.2.2 节中 A_1 面临的风险等级是 2。

同理在计算了 A_1 的其他 4 个风险值之后，也可以查出 A_1 的其他 4 个风险等级。

在获得了一个信息系统所有的资产面临的所有风险等级之后，也常以资产为横坐标、风险等级为纵坐标绘制成柱状图（或其他直观的表示形式），从而形象地展示和比较不同的资产在不同的威胁和不同的脆弱性之下，哪些是高等级风险需要及时处理（如需要立即增添新的设备、更改管理制度等），哪些是相对低等级的风险可以暂缓处理（如调整现有安全防护设备等）。决策者也能够从中了解到本组织的信息系统所面临的风险分布情况，有利于下一步进行风险控制的决策。读者将在本章案例分析中看到相关内容。

10.4　风险控制

尽管“风险分析”、“风险评估”、“风险控制”等术语在信息安全领域交叉使用的现象非常普遍，属于近义词或同义语。但在本书中，我们将风险控制定位为完成风险状况评估之后，如何转嫁、减缓直至承担风险的过程。

所谓风险控制，本质上就是在获得了信息系统所面临的风险分布情况之后，应该提出相应的解决办法（也就是安全解决方案），以规避、降低、转嫁直至承担相应的风险。“安全解决方案”是许多读者已经熟悉的语言，它是信息安全工程师以科学的数据（如上面介绍的各种赋值）为支持，充分考虑被评估单位业务发展的长远战略目标及安全投

入的成效比等因素，为用户提出的一套“量身定制”的信息系统安全建设工程计划。

在明确了一个信息系统中的各种资产所面临的各种风险值（或风险等级）之后，组织应当综合考虑风险控制成本与风险造成的影响，提出一个可以接受的风险范围。对某些资产的风险，如果风险计算值（或风险等级值）在可接受的范围内，则该风险是可以承担的，应保持已有的安全措施；如果风险计算值（或风险等级值）在可接受的范围之外，即风险计算值高于可承受风险的上限值，则该风险是不可承受的，需要采取安全措施以降低、控制风险。还有一种风险控制的方法就是确定了风险等级之后，按不同的级别进行处理，这实际上就是本书第 2 章信息安全等级保护中的内容。

安全解决方案是安全专业技术人员为用户提供的安全服务的最终体现，具有将科学和艺术融为一体的魅力。这里仅仅是抛砖引玉，给读者建议在制定安全解决方案的时候应遵循的一些原则。下面将在本章案例分析中给出“数字兰曦”的安全解决方案供读者参考。



风险控制（安全解决方案）四原则

（1）**论证充分。**要避免“围绕产品说方案”的落后思维方式。首先要明确安全解决方案不是“安全产品推销方案”。应严格遵循国家标准（如风险评估标准、信息安全等级保护标准等），获得风险控制所需要的基础数据（如风险值等）。让用户对自身信息系统所面临的安全问题有一个科学、全面、清晰的认识。

（2）**循序渐进**。在充分论证的基础上坚持“有所为、有所不为”的指导思想，循序渐进地控制风险；要让用户明确“没有绝对的安全和零风险”；要充分考虑用户现有信息系统的实际情况，避免重复建设，保护已有投资。

（3）**结合国情**。在制定风险控制方案的过程中，要结合中国的国情。中国信息安全保障工作的根本制度是实施信息安全等级保护（除非今后中国的相关法律进行了更新，见本书第 12 章《法律、法规》有关内容）。因此评估人员应当将“风险评估”与“等级保护”结合起来，要围绕提高信息系统安全等级保护水平来思考风险控制方案。要避免仅突出国际上风险控制的主流思想，而与中国等级保护制度脱节的倾向。

（4）**应急联动**。信息安全保障体系的最有效验证是面对突发信息安全事件的反应能力，也就是应急响应。因此在制定风险控制方案的过程中，也要与该组织的信息安全应急响应方案结合起来，不要出现风险控制方案与应急响应方案“两张皮”的现象。我们将在第 11 章介绍应急响应方面的基础知识。

在本章案例分析中将对风险控制方法进行剖析。

10.5　残余风险

在风险控制方案实施之后，我们对信息系统面临的风险现状进行了规避、转移和降

低，但不可能彻底消灭所有风险。因此需要在有条件的情况下，确认残余的风险状况。为此，可以进行再评估，以判断实施风险控制后的残余风险是否已经降低到可以接受的水平。残余风险的评估可以依据国家标准提出的风险评估流程实施，也可以做适当裁剪，即直接利用前面资产识别和威胁识别的结论，从脆弱性评估这个环节开始分析残余风险。

某些风险可能在选择适当的安全措施之后，残余风险的结果仍处于不可接受的风险范围之内，此时就应进一步加强相应的安全措施。

由于残余风险的评估流程和原理与前面各章介绍的内容完全相同，因此本书在此从略，只是提醒读者注意，从信息安全风险评估流程完整性的角度来讲，残余风险的评估是其中最后一个步骤。

最后作为风险评估各章的一个总结，给出风险评估各个环节的逻辑关系图，以帮助读者提纲契领式地回忆一下到此为止所介绍的各项内容，如图 10.2 所示。

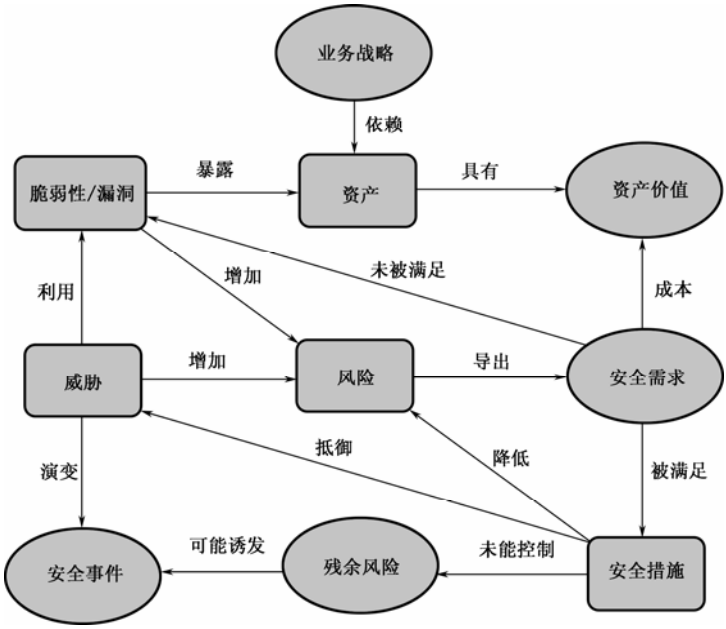


图 10.2　风险评估各个环节的逻辑关系图

10.6　风险评估案例分析

在本节中，依然以“数字兰曦”为例介绍风险计算、风险控制（安全解决方案）等内容，从而完成整个风险评估的环节。首先，对“数字兰曦”的信息环境风险、公用信息载体风险和专用信息及信息载体风险进行计算。计算方法是 10.2.1 节所介绍的“相乘法”。

10.6.1　信息环境风险计算

兰曦公司的“数字兰曦”虽然属于由中国电子工业集团行业专属的纵向垂直体系，但同时也是巴山市大型骨干企业，与当地政府的信息系统也有横向信息沟通，如税收信息就需要会聚到巴山市税务信息系统等。因此，“数字兰曦”的业务应用较为复杂、系统应用人员数量众多、区域覆盖面广，整个系统网络结构复杂、互联技术较多，对于整个“数字兰曦”信息环境风险值的计算将按子系统分解后再进行计算。针对各个子系统所处的信息环境的风险计算则单独提出，其中包括人员资产风险计算、管理制度资产风险计算和机房资产风险计算。由于本书篇幅所限，因此只是对每一类资产所面临的风险抽出有代表性的几个例子进行展示，特此说明。

10.6.2　人员资产风险计算

人员是一类特殊的资产，在信息系统中占有重要的地位，他们担负着信息系统的管理、运行维护、安全防范等各个方面的任务，覆盖的范围比较大，牵涉的面比较广。因此，对人员资产的风险评估也是异常重要的，对人员类资产的风险控制也是整个“数字兰曦”风险控制的关键因素。使用“相乘法”计算，得出的人员资产的风险值和相应的风险等级值如表 10.3 所示。

表 10.3　人员资产风险计算

序号	资 产 名 称	资产等级	威胁发生频率	脆弱性严重程度	风险值	风险等级
1	公司信息化领导小组	5	2	1	1	很低
2	公司信息中心	4	1	1	1	很低
3	分公司/研究院人员	3	5	3	2	低

10.6.3　管理制度风险计算

管理制度资产作为一类特殊的资产，也是重点评估的对象，在以往的安全事件中利用管理制度的漏洞来间接对机构信息系统的渗透和破坏屡见不鲜，因此它也是风险计算的一个必要因素。兰曦公司整体的信息系统经过长期的运营维护，已有较为完善的规章管理制度，但各个规章制度的具体内容和可操作性还有所欠缺。经过计算，管理制度风险计算如表 10.4 所示。

表 10.4　管理制度风险计算

序号	资 产 名 称	资产等级	威胁发生频率	脆弱性严重程度	风险值	风险等级
1	信息化规章管理制度	4	10	3	5	中等

10.6.4　机房风险计算

作为整个信息系统运行的基础及物理上的最外围保护措施，机房及保障设备本身的安全也是一个需要重点关注的地方。兰曦公司由于系统的分布覆盖面较广，机房建设的情况也较为复杂，作为整个系统主要机房的公司中心机房是按照国家 A 类机房建设标准进行建设的，配备了较为完善的保障设备，并在系统长期的运行维护中制定了较为完备的相关管理制度。但经过评估，仍存在部分问题需要整改。机房风险值及其风险等级如表 10.5 所示。

表 10.5　中心机房风险计算

序号	资产名称	资产等级	威胁发生频率	脆弱性严重程度	风险值	风险等级
1	中心机房	5	4	3	2	低

对信息环境其他资产也采用“相乘法”进行计算后，得出信息环境总体风险分布情况如下所述。

10.6.5　信息环境风险统计

信息环境在整个“数字兰曦”中的风险值较低，这与“数字兰曦”的建设和领导的重视有关。从表 10.6 可以看出，信息环境没有高危和中等风险，全部集中在低等级以下，因此可以得出结论：即使与这些风险相对应的安全事件确实发生了，也不会对整个信息系统造成实质的影响。

表 10.6　“数字兰曦”信息环境风险值统计

风　险　项	很高	高	中	低	很低
系统物理设备未授权访问	0	0	0	5	4
信息探测威胁	0	0	0	3	0
泄密	0	0	0	1	0
窃密	0	0	0	0	3
权限滥用	0	0	0	1	0
欺骗威胁				0	3
总计	0	0	0	10	10

10.6.6　公用信息载体风险计算

1．通信载体风险计算

公用信息载体资产是指整个信息系统的基础网络平台，但不包括信息系统各子系统的专用设备。公用信息载体资产为整个信息系统的信息提供传输通道，对信息进行安全检查并对其流向进行控制，同时也对信息进行最初始的采集、加工和最后的处理、应

用；涉及信息系统信息的采集、处理、传输、存储和应用的各个环节，因此保障公用信息载体资产不被非法访问和破坏是保障整个信息系统安全和最终的信息安全的关键点。通信载体资产情况参见表 7.12，由于篇幅原因，表 10.7 仅给出了一个三层交换机风险计算的结果。

表 10.7　通信载体风险计算

序号	资 产 名 称	资产等级	威胁频率	脆弱性严重程度	风险值	风险等级
1	三层交换机 CISCO 6506	5	42	4	7	很高

2．安全防护设备风险计算

安全防护设备资产参见表 7.13，由于篇幅所限，这里仅给出 1 台防火墙风险计算的结果，如表 10.8 所示。

表 10.8　防火墙风险计算

序号	资 产 名 称	资产等级	威胁频率	脆弱性严重程度	风险值	风险等级
1	FORTIGATE（美国）	5	30	3	6	高

3．公用信息载体风险统计

最后是公用信息载体（通信载体、安全防护设备）的风险统计，如表 10.9 所示。

表 10.9　公用信息载体风险统计

风　险　项	很高	高	中	低	很低
网络操作系统故障	1	1	2	2	4
总计	1	1	2	2	4

在表 10.9 中，公用信息载体风险值很高的 CISCO 6506 这一项应特别注意（见表 10.7），这是由于没有设定三层路由，VLAN 之间控制手段薄弱，从而对“数字兰曦”的正常运行造成潜在的危害。风险值高的一项对应于表 10.8。FORT1GATE 存在旁路迂回的攻击风险，需要适时调整。风险值低的有两项，都属于网络操作系统故障，会对“数字兰曦”造成潜在的影响，但不会对兰曦公司造成不可弥补的损失。

10.6.7　专用信息及信息载体的风险计算

“兰芯”子系统是从 2004—2006 年由国内大型软件开发商“快帆”公司承建开发的，整个系统的开发遵循中国电子工业集团“统一平台、统一数据库、统一网络”的规范。系统主要包括营销管理、现代物流、客户关系管理、供应链管理、供应商管理、人力资源、生产管理等八个方面的应用。

作为兰曦公司最重要的生产经营系统，“兰芯”子系统使用范围覆盖了 12 家分公司和 1 家研究院及全国 145 个销售网点，所有的业务应用及业务数据都集中在公司中心机

房的服务器，呈现出明显的应用大集成和数据大集中的特点。通过“兰芯”子系统的应用，实现了为全国数百个客户提供从订货到送货全流程的优质服务；实现了客户与市内工、农、建、信用合作社、邮政 5 家银行中任意 1 家银行进行货款交易的实时扣划，加快了货款回笼，方便了客户货款支付；营销数据实时汇集到公司各级管理部门，实现了各级领导干部和管理人员随时了解、分析行业经济运行情况，提高经营决策和运行调控的效率的目标；通过对供应链的一体化管理，实现了以市场为导向优化资源配置、提高效率、降低成本、提升效益的目的，表 10.10 是采用“相乘法”对“兰芯”子系统（双机备份）进行风险计算的结果（由于篇幅原因，其他风险计算从略）。

表 10.10　“兰芯”子系统（双机备份）风险计算结果

序号	资 产 名 称	资产等级	威胁发生频率	脆弱性严重程度	风险值	风险等级
1	“兰芯”子系统应用服务器及热备应用服务器”（DA01）	5	28	4	6	高

同理，我们可采用“相乘法”对“兰芯”子系统各专用信息及信息载体资产进行了风险值计算，其总体风险统计情况如表 10.11 所示。

表 10.11　“兰芯”子系统风险统计

风　险　项	很高	高	中	低	很低
信息欺骗	0	0	2	1	4
拒绝服务	0	6	1	2	2
总计	0	6	3	3	6

“兰芯”子系统是“数字兰曦”的核心业务子系统，其系统中高风险值有 6 个占整体风险值的 60%，这些潜在的安全威胁一旦发生，会对兰曦公司的信息系统造成较为严重的影响，会使兰曦公司正常业务中断。中等风险值的安全事件有 3 个，占整体风险值的 30%，这些潜在的安全威胁一旦发生会对“数字兰曦”造成一定的影响，但此影响是可以弥补的，不会造成重大损失。低或很低的风险共有 9 个，不会对“兰芯”子系统产生很大影响。

10.6.8　风险计算报告

与资产识别类似，本章结束之后也需要出具《风险计算报告》。该报告的主体包括被评估单位面临的风险值和风险等级等。下面仍以“数字兰曦”为例给出该报告的格式，仅供参考。

错误！

“深海”信息安全测评中心

“数字兰曦”风险计算报告

摘要
目录
图标目录
报告审批（授权签字）及日期
1　撰写依据
2　术语解释
3　风险计算方法
4　“数字兰曦”系统风险概述
5　“数字兰曦”风险值及风险等级
5.1　“兰芯”子系统风险值及风险等级
5.2　“兰剑”子系统风险值及风险等级
5.3　……
6　附录

10.6.9　风险控制示例

通过对兰曦公司专属子系统——“兰芯”子系统的风险值分析，我们对“兰芯”子系统的数据安全、应用安全和主机安全提出以下风险控制措施（注意，这里没有涉及网络安全和物理安全的内容，因为这些内容属于公用信息载体和信息环境）。顺便指出，下面所述的安全风险控制措施有不少可以参照本书前半部分中数据安全测试技术、主机安全测试技术等方面的条款来给出。因此读者应当将本书中所介绍的安全测评与风险评估技术融会贯通。

1．数据安全风险控制措施

（1）“兰芯”子系统拥有的管理数据、各种鉴别信息和用户数据在传输过程中应保证数据的完整性不受到破坏。

（2）“兰芯”子系统上的各种网络设备、操作系统、数据库管理系统和应用系统要防止对身份鉴别信息的未授权访问。

2．应用安全风险控制措施

（1）在核心应用业务中，通信双方在进行通信时，如果一方在一段时间内未作任何响应，可以考虑通过一种机制让另一方能够自动结束会话，以避免长时间等待造成两者

的通信失去保密性。

（2）在核心应用业务中，在进行数据交互时，可以考虑为数据源发者或接收者提供数据源发证据的功能，即数据标识。

（3）核心应用业务子域中的 Web 服务器 Apache Tomcat 3.3.1 及之前的版本，可允许远端攻击者获得敏感信息，如果远端攻击者送出 URL 请求，并加上空位的字节（如 GET/.jsp HTTP/1.0），服务器将回应目录列表给攻击者。建议升级到最新版本的 Tomcat。

（4）核心应用业务子域中的 Web 服务器 Apache，在处理某种大模块的编码 HTTP 要求时，会允许远端攻击者执行任意程序，建议升级到最新版本的 Apache。

（5）核心应用业务子域中的 Web 服务器 Apache HTTP Server 的 mod_alias 及 mod_rewrite 模块存在缓冲区溢出弱点，攻击者可以创建特定的配置文件来造成拒绝服务或执行任意程序，建议升级到最新版本的 Apache。

3．主机安全风险控制措施

（1）在核心应用业务中应对重要信息资源和访问重要信息资源的所有主体设置敏感标识。同时制定强制访问控制策略，其策略的范围应涉及与重要信息资源直接相关的所有主体、客体及它们之间的操作，强制访问控制的粒度应达到主体为用户级，客体为文件、数据库表级。

（2）在核心应用业务中，安全审计要对各种安全记录数据进行分析，并可以生成审计报表。

（3）在核心应用业务中，可以考虑通过软件方法设置一些重要、敏感资源报警的阈值，在资源使用超过规定数值时发出报警，实现一些异常进程的监控，限制操作人员运行非法进程，同时可以对主机的所有账户进行监控，使得对一些重要的账户不能删除和更改。一旦有如上的操作，要进行严格的日志管理。

（4）核心应用业务服务器上安装的 Windows 2000 系统存在“空口令”配置，会让攻击者远程上传任意的恶意文件至系统内。建议兰曦公司制定一套比较标准的口令配置策略，如口令长度，让口令包括数字、大小写字母与特殊符号相结合，具有一定的复杂度。

（5）核心应用业务中的 MSSQL 2000 和 MSDE 的数据一致性校验存在缓冲区溢出时，允许以数据库管理员或者数据库成员的身份执行任意代码，因此建议利用较好的杀毒软件阻止 sqlhello.exe 和 nc.exe 等溢出工具的运行。

（6）Oracle 数据库中，本地用户（最低权限的用户）可以通过 ctxsys.driload package 提升用户的权限。建议如果不需要 ctxsys 账号，可在 Oracle 下执行删除账号命令删除 ctxsys 账号，或者通过命令控制此用户权限。

（7）对 Windows 2000，匿名的攻击者可以建立一个包含恶意程序的信息，并发送到 Windows 2000 系统中，造成缓冲区溢出的现象。解决这个问题可以通过微软推出的 KB902400 修正程序进行修正。

（8）对 Windows 2000，由于微软 Windows 操作系统 Plug and Play（PnP）功能的输入检查不够完善，攻击者可能利用恶意的程序或装置来使其缓冲区溢出并执行任意的程序；本地端的攻击者也可以利用这个弱点来提升自己的权限。建议参考 Microsoft Security Bulletin MS05-039，安装补丁程序。

（9）对 Windows 2000，Microsoft Distributed Transaction Coordinator（MSDTC）有缺陷，其弱点发生于 msdtcprx.dll 中的 CRpcIoManagerServer::BuildContext 函数。此时，远端攻击者可以对 BuildContextW()函数发送一个大的请求（超过 4KB），略过大小范围的检查，导致 MSDTC 服务停止。此问题可以通过微软推出的 KB913580 修正程序进行修正。

（10）Windows 2000 服务器的服务存在缓冲区溢出弱点，远端攻击者可以经由 TCP 通信端口 139 或 445 发送特别制作的信息让服务器回应造成缓冲溢出，进而执行任意程序。此问题可以通过微软推出的 KB921883 修正程序进行修正。

（11）在应用业务中，攻击者可以利用 Windows SMB 的漏洞，由远端发起拒绝服务攻击，此问题可以用 MS06-063 取代 MS06-035。

（12）分公司服务器存在开放 139 端口现象，攻击者可以扫描得到开放此端口的服务器信息，获取共享资源。建议关闭 139 端口。

（13）Oracle 8i 版本 CREATE DATABASE LINK 存在一个缓冲区溢出弱点，应将 Oracle 8i 第二个版本升级到 8.1.7.4。

（14）Windows 2000 的 Scheduler 在检查缓冲区域时缺乏适当的验证，这样会导致一个缓冲区溢出的弱点。攻击者可以架设恶意的网站或恶意的 E-mail 来引诱使用者去浏览，一但使用者浏览了这个信息，攻击者便可以取得使用者的权限，执行任意的程序。控制措施是可以参考 Microsoft Security Bulletin MS04-022，安装 KB841873 安全补丁程序，或直接安装 Update Rollup 1 for Windows 2000。

（15）Windows 2000 Server Message Block 所提供的服务对使用者输入的资料缺乏足够的检查，攻击者正可以利用该通信协定传送一个异常格式的信息，并使用系统的权限执行任意的程序。控制措施可以参考 Microsoft Security Bulletin MS05-027，安装 KB896422 补丁程序。

（16）对 Windows 2000，若连线到分享打印机，则可以传送异常的信息到分享的打印机上，导致 Print Spooler 服务的缓冲区溢出。攻击者可以使服务器宕机并在服务器上执行任意的程序。解决此问题建议参考 Microsoft Security Bulletin MS05-043，安装相应补丁程序。

（17）Windows 2000 允许远端攻击者揭露应用程序或事件记录。远端攻击者在空连接（NULL sessions）情况下可以利用 named pipes 及 Microsoft Remote Procedure Call framework（MSRPC）列举出事件记录。解决此问题可以参考 Microsoft Upgrade Update Rollup 1 for Windows 2000，安装 KB891861 Hotfix。

在这里罗列了众多的风险控制措施，其实是想向读者传递这样一个信息，即如果您是遵循实事求是的态度做出的安全解决方案，那么您会发现其中有很大部分的安全措施是通过调整现有设备配置、进行补丁升级、加强管理制度等来实现的，只有少部分关键的风险，需要增添新的设备。事实上，在进行风险评估，特别是制定风险控制方案的时候，作为一个有专业水准同时又具有职业道德素养的工程师来说，应该首先利用好用户现有的各种设备（包括软件系统），为他们制定“安全加固”方案，而不是每次都推翻前人的建设成果。在此基础上，进行残余风险分析，若发现有部分风险无法通过现有设备的调整进行控制，再制定“安全整改方案”或“安全升级方案”，从而保护用户的已有投资。从长远的发展战略来讲，也有利于中国自身信息安全产业链和服务链的健康成长。下面是对“兰芯”子系统残余风险的分析。

4.“兰芯”子系统残余风险分析

根据兰曦公司提供的资料，“兰芯”子系统的安全等级为第 3 级，通过核心应用业务子域的安全现状分析和国家等级保护第 3 级的有关标准，分析得出安全需求，根据在线渗透测试和现场漏洞测试出的弱点，结合兰曦公司的实际，对数据安全、应用安全和主机安全的建设提出建设方案，通过对核心应用业务子域实施建设方案，对核心应用业务子域“兰芯”子系统的残余风险得到有效控制。

通过图 10.3，可以看出通过实施核心应用业务子域的安全建设方案，数据安全可以完全达到满足核心应用业务子域的安全建设需求，应用安全可以达到 40%的安全需求，主机系统安全可以达到 69.2%的要求。从而将重要业务风险控制在国家等级保护中第 3 级的相关标准内。

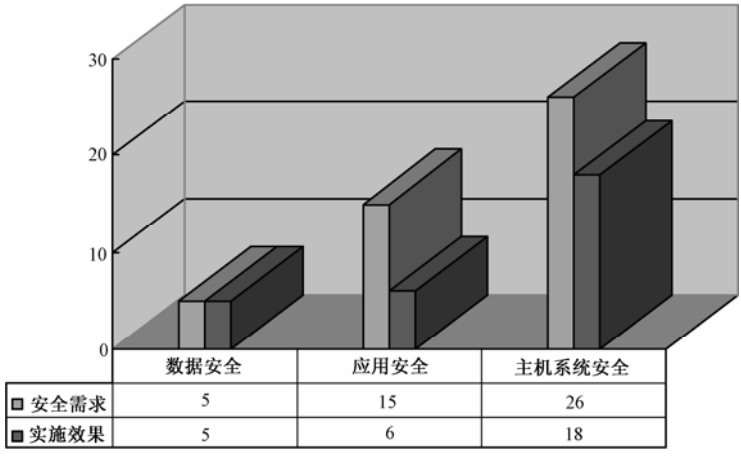


图 10.3　核心应用业务子域建设方案预期效果图

由于篇幅所限，关于兰曦公司“信息环境风险控制”、“公用信息载体风险控制”等相关内容从略，但其基本思想已经通过“兰芯”子系统的风险控制措施予以展示，请读

者在自己的学习、工作中举一反三。

10.6.10　风险控制计划

风险控制计划也就是人们常说的“信息安全解决方案”。**一个科学、合理的“安全解决方案”应该是建立在风险评估基础上的。**此外，测评工程师也应该结合组织的信息系统对等级保护的要求来综合考虑这个安全解决方案。

风险控制措施分析和残余风险识别结束之后，也需要出具《风险控制计划》。该计划的主体包括向被评估单位建议的风险控制措施和残余风险分析等。由于前面已经讨论了“兰芯”子系统的风险控制措施及剩余风险分析方法，因此下面仍以“数字兰曦”为例，给出该报告的格式，仅供参考。

“深海”信息安全测评中心

“数字兰曦”风险控制计划

摘要

目录

图标目录

报告审批（授权签字）及日期

1　撰写依据

2　术语解释

3　“数字兰曦”系统风险控制概述

4　“数字兰曦”风险控制与残余风险分析

4.1　“兰芯”子系统风险控制与残余风险分析

4.2　“兰剑”子系统风险控制与残余风险分析

4.3　……

5　附录

最后，罗列出风险评估工作结束后应该向用户提交的相关文档，供读者参考。



风险评估文档一览表

作为“风险评估”这部分的结尾，我们给出测评工程师在进行风险评估工作中应该向用户提供的各种技术报告、清单、列表或记录。这些计划、技术报告、清单、列表或记录可以融入到本书所建议的《资产识别报告》、《威胁识别报告》、《脆弱性识别报告》、《风险计算报告》、《风险控制计划》等文档之中。读者也可以在此基础上撰写一个总体性的《风险评估报告》。

（1）风险评估计划：阐述风险评估的目标、范围、人员、评估方法、评估结果的形式、实施进度和所需资源等；

（2）风险评估程序：明确评估的目的、职责、过程、相关的文档要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据；

（3）资产识别清单：根据组织在风险评估程序文档中所确定的资产分类方法进行资产识别，形成资产识别清单，明确资产的责任人/部门；

（4）重要资产清单：根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度和责任人/部门；

（5）威胁列表：根据威胁识别和赋值的结果，形成威胁列表，包括威胁名称、种类、来源、动机及出现的频率等；

（6）脆弱性列表：根据脆弱性识别和赋值的结果，形成脆弱性列表，包括具体脆弱性的名称、描述、类型及严重程度等；

（7）已有安全措施确认表：根据对已采取的安全措施确认的结果，确认已有安全措施确认表，包括已有安全措施名称、类型、功能描述及实施效果等；

（8）风险评估报告：对整个风险评估过程和结果进行总结，详细说明被评估对象、风险评估方法、资产、威胁、脆弱性的识别结果、风险分析、风险统计和结论等内容；

（9）风险控制计划：对评估结果中不可接受的风险制定风险控制计划，选择适当的控制目标及安全措施，明确责任、进度和资源，并通过对残余风险的评价以确定所选择安全措施的有效性；

（10）风险评估记录：根据风险评估程序，要求风险评估过程中的各种现场记录可复现评估过程，并作为产生歧义后解决问题的依据。

10.7　本章小结

- 风险分析的概念
- 风险值计算的三个环节
- 用相乘法计算风险
- 风险定级
- 风险控制的概念
- 风险控制的四个原则
- 残余风险的评估环节

尾声：“勇敢”的反面是什么

两强相遇勇者胜——可见“勇敢”的力量。

“勇敢”的反面是什么？当然是“怯懦”了——你是不是毫不迟疑地这样答道？

是的，“两强相遇勇者胜”，反过来说难道不就是“两强相遇怯者败”吗？“勇敢”与“怯懦”泾渭分明，人们可以很容易地把两者清楚地区分开来。

但是，且慢……

假设，有那么一个“旱鸭子”，他说他要徒手横渡英吉利海峡；有那么一个会严重高原反应的家伙，他说他要徒手攀登珠穆朗玛峰。如此，他们绝对不是“怯懦”之辈吧，他们应是“怯懦”的反面吧？

“怯懦”的反面？那他们就是“勇敢”了？不！他们也不属于“勇敢”，他们应该属于的恰恰应该是“勇敢”的反面，而这个反面，并非“怯懦”，这个反面，就叫做“鲁莽”。

人们很容易分清“勇敢”与“怯懦”，却常常混淆“勇敢”与“鲁莽”，常把“鲁莽”当作“勇敢”。人们的这种糊涂在面对其他范畴问题时也常常发生。

人们对待“风险”的态度，恰恰就在“勇敢”和“鲁莽”之间。

当我们高喊无所畏惧的时候，让我们仔细想想：

“勇敢”其实是，有所畏惧，有所准备，然后才变得无畏；

“鲁莽”分明是，无所畏惧，无所准备，然后就奔向无望。

所以，知道“怕”，并非坏事。

观感

（1）风险定级与信息系统的安全定级是什么关系？

（2）风险等级高的系统一定对应于高安全等级的系统吗？为什么？

（3）查阅相关科技文献，看一看还有哪些流行的风险值计算方法。

（4）请在第 7、8、9 章的基础上，计算“兰芯”子系统的风险并给出其风险等级。然后在此基础上撰写《“兰芯”子系统风险计算报告》和《“兰芯”子系统风险控制计划》。

第 11 章

应 急 响 应





19 世纪消防车模型

凡事预则立，不预则废。

——《礼记·中庸》

序幕：虚拟社会的消防队

从公开的报道来看，尽管在 1983 年、1984 年和 1987 年已经发生过数起针对 ARPAnet、美国太空总署（NASA）和军用专网的攻击，“黑客第一人”Kevin Mitnick 也被 FBI 送去享受免费却没有自由的午餐了，但由于这些攻击并未造成较大损害，所以一直没有引起人们过多的关注。

1988 年 11 月 2 日，美国 Cornell 大学的研究生 Robert T. Morris，他也是美国国家安全局（NSA）计算机安全首席专家 Robert Morris 之子，向 ARPAnet 传送了那段仅有 99 行代码的著名程序，虚拟世界的烽火台上终于升起了第一股狼烟。同年年底，互联网的发源地——美国国防部高级研究计划署（DARPAR）随即拨出专款在著名的卡内基·梅隆大学软件工程研究所（Carnegie Mellon University/SEI）成立了一个名为“计算机应急响应协调组”（CERT/CC）的机构。那一年，CERT/CC 只有 3 名正式员工，仅仅处理了 5 起安全事件…… 到了 2001 年，CERT/CC 已经拥有 50 余名专家，第一季度应急处理的安全事件就有 7047 起。

2000 年 10 月，中国成立了“国家计算机网络应急技术处理协调中心”（CNCERT/CC）。2003 年，美国组建了隶属国土安全部的计算机应急响应组织 US-CERT，同时英国 CERT、法国 CERT、德国 CERT、日本 CERT、加拿大 CERT…… 纷纷成立了虚拟社会的“消防队”。

要点：本章结束之后，读者应当了解和掌握

- 应急响应与应急响应计划是什么关系？
- 应急响应的三个关键环节是什么？
- 如何制定应急响应计划？
- 为什么需要进行应急演练？

11.1　应急响应概述

“有备无患”是人人都熟悉的语言。在面对各种突发事件的时候，是否处变不惊，是否应对得当，是否能化险为夷…… 是对一个政府、组织及个人应变能力的严峻考验。

> 应急响应（Emergency Response），指组织为了应对突发/重大信息安全事件的发生所做的准备及在事件发生后所采取的措施。

随着读者对风险评估知识的了解，现在终于能够向读者介绍信息安全保障工作中一个非常重要的领域了，这就是信息安全应急响应。本书前面各章所介绍的内容，都可以从应急响应这个角度加以检验。然而安全事件突如其来，如何做到“能应急”而不是“干着急”呢？上面所说的“有备无患”的“备”字，实际上就是一个“本子”，即“应急响应计划”。

> 应急响应计划（Emergency Response Plan），指组织为了应对突发/重大信息安全事件而编制的，对包括信息系统运行在内的业务运行进行维持或恢复的策略和规程。

1．应急响应和应急响应计划

应急响应和应急响应计划好比“作战行动”和“作战计划”，两者是相互补充与促进的关系。

首先，应急响应计划为信息安全事件发生后的抢险救灾工作——应急响应提供了指导策略和详细的抢险流程，否则，抢险救灾工作将陷入混乱，这些毫无章法的抢险救灾行动只能是“忙中添乱”，有可能造成比信息安全事件本身更大的损失；其次，应急响应必将会发现事前应急响应计划的不足之处，从而吸取教训，进一步完善信息安全应急响应计划并等待下一次安全事件的检验……

因此，制定应急响应计划与应急响应是一个循环反复、不断升华的过程，如图 11.1 所示。

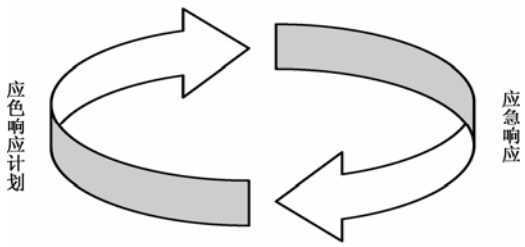


图 11.1　应急响应计划与应急响应关系

2．应急响应和风险评估

应急响应和风险评估是一个有机的整体。事实上，一个全流程的风险评估工作应当包括对组织的应急响应能力的评估。如果说两者之间有什么微小的差异的话，那就是风险评估注重的是组织“平时”的信息安全，是长期性的、渐变的；应急响应注重的是组织“战时”的信息安全，是短暂的、突发性的。请注意，这里没有使用“常态性”和“临时性”这一对词来区分两者之间的差异，因为我们认为无论是风险评估还是应急响应，从信息安全意识来讲，都应当是常态性的。例如，在突发自然灾害降临的瞬间，那些平时既有防灾意识，又经常进行应急演练的组织所遭受的损失就相对较小。

11.2　应急响应计划

“地震发生后，我们立即启用了应急预案……”。这句话是有关“5 • 12”汶川大地震新闻报道中出现得最频繁的语言之一。

在应急响应所涉及的各种活动中需要抓住应急响应计划的三个关键环节，即“计划的准备、编制和实践”形成了一个不断反馈、螺旋上升的闭环，**应急响应的基础是计划的准备，应急响应的依据是计划的编制，应急响应的核心是计划的实践**。

（1）计划的准备阶段：所谓“不打无准备之仗”。在从事任何一项工作之前都要弄清楚“为什么”和“是什么”，应急响应也不例外。应急计划的准备就是指应急响应需求分析和应急响应策略的确定。需求分析和策略的确定是建立在风险评估的基础之上，并且紧紧围绕着组织的业务战略来展开的。

（2）计划的编制阶段：在明确了应急响应的需求和响应策略的基础上，应当将这些需求和策略细化成应急响应的各项措施，也就是编制应急响应计划文档。

（3）计划的实践阶段：俗话讲“计划赶不上变化”，如果不对应急响应的参与人员按照计划进行培训、演练（实战）和更新，就会落入“纸上谈兵”的境地，应急计划也就失去了存在的价值，甚至成为了一个“有害无益”的计划。

图 11.2 是应急响应计划的工作流程图。

接下来对这个框图中的有关概念做一个介绍。

11.2.1　应急响应计划的准备

如上所述，计划的准备阶段实际上就是应急响应的需求分析和响应策略的选择阶段，它包括了风险评估、业务影响分析和制定应急响应策略三部分内容。由于读者已经熟悉了风险评估的内容，所以下面介绍业务影响分析，这也是计划准备阶段最核心的部分。

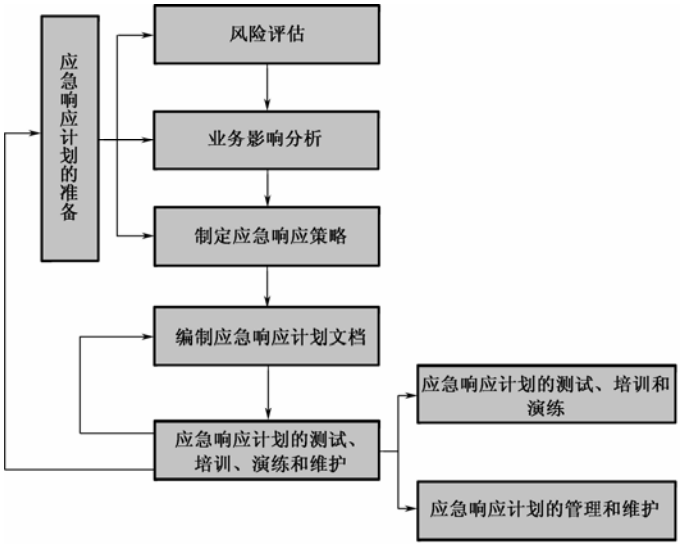


图 11.2　应急响应计划的工作流程图

业务影响分析（BIA，Business Impact Analysis），是指对业务功能及其相关信息系统资源进行分析，评估特定信息安全事件对各种业务功能的影响的过程。

读者可能已经注意到，BIA 所要求完成的工作与前面第 7 章至第 10 章的许多内容相似。事实上，BIA 包含了两层含义，一是在风险评估的基础上分析各种信息安全事件发生时对业务功能可能产生的影响，也就是在风险评估相关章节中反复强调的“面向业务的风险评估”，或者更直接地讲，就是风险分析的结果。二是 BIA 还有进一步的要求，那就是在风险分析的基础上确定应急响应的恢复目标。

那么什么是应急响应的恢复目标？怎样确定那些需要恢复的目标？如何度量目标确实有效地恢复了呢？

恢复目标的确定，实际上就是在风险评估中所识别和整理出来的“重要资产清单”。为了科学地衡量目标是否有效恢复，需要进一步确定以下两点。

（1）**优先顺序**：关键业务功能及恢复的优先顺序。也就是模拟整个组织的业务全面中断之后，最先应该“抢修”的是哪个子系统。例如，在战争中，遭受打击的指挥机关和通信枢纽的恢复优先顺序最高；而在地震发生之后，抢救人民的生命（恢复目标）是第一优先；银行信息系统宕机后，如果电力供应正常，那么核心数据库的恢复也许是第一优先等。

（2）**时间和范围**：即恢复时间目标（RTO，Recovery Time Object）和恢复点目标（RPO，Recovery Point Object）的范围。模拟业务停顿随时间而造成的损失，进而确定对组织而言比较适合的 RTO 及 RPO。


RTO 和 RPO 的确定是一个综合衡量各种因素的过程，包括业务重要性、恢复难度、恢复成本等因素。

（1）**业务重要性。**业务越重要，相应的 RTO 的值就越小。从用户的角度来讲，当然希望所有的 RTO 值都趋于零，但这在应急响应中是办不到的，否则就落入了“什么都重要等于什么都不重要”的怪圈。因此需要和用户事先沟通（沟通的顺序应该以该组织的决策层和信息系统管理部门为主，兼顾各业务应用部门），并从风险控制和承担剩余风险（见本书第 10 章风险评估相关内容）的角度来量化分析 RTO 和 RPO。

（2）**恢复难度。**恢复难度是确定 RTO/RPO 时需要考虑的另一个因素。例如，对于那些业务连续性要求很高的单位（如证券交易信息系统、电网信息系统等），就必须考虑使用双机热备（hot standby）等不间断恢复技术来确保组织核心业务不受重大影响，接下来再考虑查找故障原因，恢复主服务器功能等工作。需要指出的是，确定金融行业的 RTO/RPO 指标相对容易，因为金融行业对业务连续性历来就非常重视，有着较为完整的历史数据和案例，可供我们进行分析，此外，诸如 Gartner、IDC 等国际知名咨询公司也提供相应的参考数据，可供我们分析和确定 RTO/RPO。这是应急响应服务规范化的一种体现。对一般的组织机构而言，RTO/RPO 的确定则需要决策层提供参考意见。建议此时不要过多地“走群众路线”，即询问所有的用户，否则又会陷入“一切都重要等于一切都不重要”的怪圈之中。



> 据日本《读卖新闻》报道，日本政府由总务省牵头，在 2006 年举行了大规模的反电子攻击演习，以检测政府部门及包括航空公司和金融机构在内的民间企业的应急响应能力。这是日本首次由国家主导，经由计算机网络进行实际的反电子攻击演习。报道指出，日本总务省的演习计划是对航空公司处理预约机票和金融机构处理网上业务的计算机进行攻击演习，同时也邀请日本的通信公司及网络公司等参加演习，具体的演习方式是设立模拟电网服务器，然后由专家展开网络攻击以调查各单位如何因应急修复所需花费的时间。

（3）**恢复成本。**恢复成本是 BIA 乃至整个应急响应计划编制工作中的一个非常重要的部分。RTO/RPO 的恢复成本实际上就是应急响应计划中的“所需资源”。需要由应急响应服务机构和组织的管理层反复协商，最后确定“有多少钱，先办哪些事，能办多少事”。这里的“钱”只是一个代名词，实际上包括应急响应过程中动用的各种人力、物力等资源。

现在介绍应急响应计划准备阶段的最后一个内容——应急响应策略。顾名思义，所谓策略（policy），就是方法。对于一个管理规范的组织而言，策略应该从组织的信息安全战略（strategy）中衍生出来，从而保证该组织信息安全管理的整体一致性。

应急响应策略提供了在由于信息安全事件的发生（如系统宕机、网络瘫痪等）而导致业务中断的情况下，如何快速、有效地恢复信息系统运行的指导思想，用于指导、设

计应急响应计划的详细工作流程。

 和前面介绍的对资产、威胁和脆弱性等进行赋值一样，应急响应策略也可以量化。在制定应急响应策略的时候，可根据 BIA 的分析结果（实质上就是根据业务重要性/连续性的分析）对 RPO/RTO 进行分类，如按照“不间断、短时中断、可容忍的中断”等来划分，甚至可以进一步定量划分为“秒/分/小时/天/周”，然后确定对应的应急响应策略。在工程实践中，最常用的响应策略其实就是从快到慢的“I 级响应”、“II 级响应”、“III 级响应”和“IV 级响应”，并对每一级响应提出所需的资源（我们将在 11.2.2 的应急响应计划中详细介绍其含义）。但策略本身实际上是一门艺术，就如同在社会科学领域里经常看到的“斗争策略”一样，它反映了应急计划的制定者/执行者在预防信息安全突发事件方面的想象力和执行力。顺便指出，有进一步研究兴趣的读者可以参考 GB/T 20988—2007《信息安全技术 信息系统灾难恢复规范》等国家有关标准要求。

尽管应急响应扮演的是“消防队”的角色，首要考虑的是如何在尽量短的时间内“扑灭”安全事件。但一个好的应急响应计划也要考虑成本效益问题，因为在信息时代，应急响应是常态性的安全保障工作之一，必须要算经济账。因此，一个组织应确保有合理的人员和资金投入来执行所选择的策略。应进行成本效益分析，如在预算中考虑与应急响应有关的软件、硬件等设备更换，备用节点、应急演习等方面的费用，以确定最佳的应急响应策略。

需要指出的是，无须在策略制定阶段详细讨论应急响应流程的各种工作细节，策略仅仅是制定响应流程的“原则”，在实际的应急响应工作中，甚至无须专门输出一个《应急响应策略》文档，而要把它融入到《应急响应计划》之中。

11.2.2　应急响应计划制定中应注意的问题

在完成了应急响应计划的准备工作，也就是了解了一个组织的应急响应需求并确立了对应的响应策略之后，接下来应该在此基础上开始着手计划的编制。对于初次接触应急响应计划编制的读者而言，要注意以下 3 个矛盾的统一。

1．通用性和特殊性

对于初学者而言，也许最好的方式就是在网上查阅如《国家突发公共事件总体应急预案》、《国家通信保障应急预案》等资料，然后根据本单位实际情况进行“裁剪”。从管理的角度来讲，一个组织机构层次越高，应急计划就越应该具备通用性，而业务工作越单一的部门，应急计划就越应该具备特殊性。

2．灵活性和规范性

计划越详细，执行过程就越规范，但也就越缺乏灵活性。一个可行的方式是，根据对以往历史事件的分析，对于那些出现频率较高或者一旦发生就会严重影响业务连续性

的安全事件，制定比较详细的应急响应步骤，同时对较少发生或尚未发生的安全事件的应急响应步骤保留一定的灵活性，以便在今后的工作中予以充实。

3．可操作性和系统性

应急计划不是为了应付检查，而是为了在安全事件发生后真正能够应急。尽管我们始终强调在从事信息安全保障工作中（包括应急响应）要有系统科学的思想，但读者不应将其理解成系统性就是越复杂越好。事实上，应急响应计划不仅是为应急响应的专家组制定的，也是为那些对信息安全事件不熟悉的人员制定的。因此，计划应明确、简洁、易于在紧急情况下执行，并尽量使用应急检查列表和可操作的流程。

11.2.3　应急响应计划的制定

应急响应计划应包含总则、角色及职责、预防和预警机制、应急响应流程、应急响应保障措施和附件 6 个基本要素。下面分别进行简要阐述。

1．总则

总则部分实际上就是简要回答“为什么”、“凭什么”、“有什么”和“如何做”。通常这部分包括编制目的、编制依据、适用范围和工作原则。

（1）编制目的：简要介绍制定信息安全应急响应计划的原因和目标，为本计划的使用者简要回答“为什么”需要该计划的问题。

（2）编制依据：说明编制信息安全应急响应计划的依据。供参照的依据包括（但不限于）国家有关信息安全应急响应的相关标准、政府或企业制定的有关突发公共事件应急响应的文件、本单位突发公共事件应急响应计划、本单位信息安全保障工作相关文件等。为本计划的使用者回答“凭什么”的问题。

（3）适应范围：说明计划的作用范围，解决哪些问题。本计划同使用者回答“有什么”的问题。凡是不属于该计划所罗列的其他安全问题，就不在解决范围之内。举例而言，如果安全事件是由产品质量造成的，那么对相关厂商的责任追究就可以不包含在应急计划之中，而是由另外的方式（如合同）来体现。应急响应更要体现轻重缓急的应急特点。

（4）工作原则：确定应急响应计划组织和实施原则。阐述应对安全事件的准则。为本计划的使用者回答“如何做”的原则。要简明、扼要、易懂。

2．角色及职责

应急响应是日常工作的有机组成部分，因此应结合本单位日常行政/技术机构建立信息安全应急响应的工作机构，并明确其职责。通常由该单位分管信息化建设的主管出任应急响应机构的负责人。如果该单位是属于那种“信息安全敏感型”部门，换言之，信息安全事件等同于通常意义的安全事件如电信企业等，则建议由第一领导出任应急响应机构的负责人。

应急响应的工作机构由管理、业务、技术和行政后勤等部门的人员组成，一般来说，按角色可划分为 5 个功能小组——应急响应领导小组、应急响应技术保障小组、应急响应专家小组、应急响应实施小组和应急响应日常运行小组。人员配置的原则是：分配到相关小组中的人员在正常条件下负责的也是相同或类似的工作。例如，应急响应领导小组的人员应当是该单位负责信息化工作的领导和信息中心的负责人；应急响应技术保障小组的成员应当以该单位信息中心的技术人员为主；应急响应专家小组则可以由负责该单位日常安全服务的机构中的专家组成；等等。

特别需要指出的是，应急响应计划的组织实施必须在应急响应领导小组的统一指挥下开展，因此，计划是否可行的最终决定权是由领导小组审核批准的。应急领导小组的职责如下：

（1）对应急响应工作的承诺和支持，包括发布正式文件、提供必要资源（人、财、物）等；

（2）审核并批准应急响应策略；

（3）审核并批准应急响应计划；

（4）批准和监督（或指挥）应急响应计划的执行；

（5）启动定期评审、修订应急响应计划；

（6）负责组织的外部协作工作。



由于应急响应是和突发安全事件所造成的灾难“争时间、抢速度”，所以可聘请权威技术机构的专家协助应急响应工作，也可委托具有相应资质的专业技术服务机构承担应急响应部分或全部工作，这实质上也是“风险外包”的一种方式。图 11.3 为应急响应工作机构图。

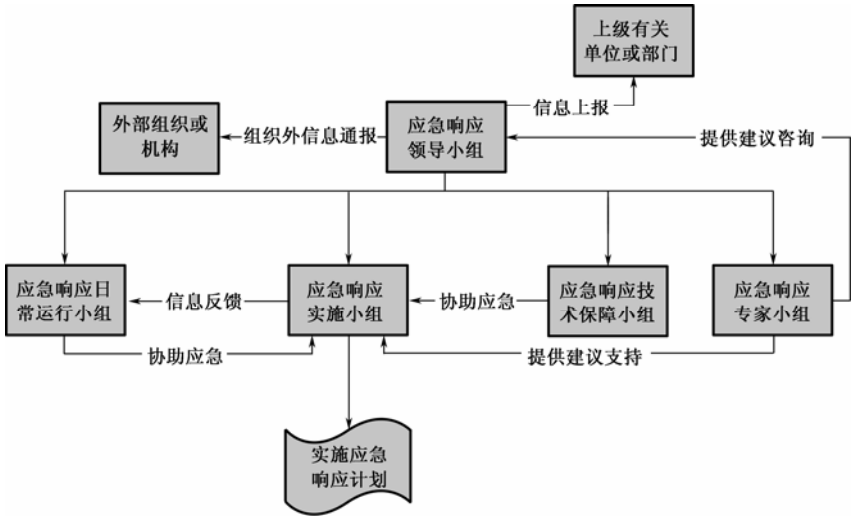


图 11.3　应急响应工作机构图

3．预防和预警机制

预防和预警机制是一种防御性的方法，即所谓的“将安全隐患消灭在萌芽状态之中”。重视信息安全事件的预防/预警，比信息安全事件发生后进行应急响应更好。在预防机制中，最常见的措施（当然远远不仅限于）就是进行容灾备份。有兴趣的读者可以参阅《信息系统灾难恢复规范》等国家的相关标准。根据本单位实际情况所采取的预防机制应被记录在应急响应计划中，同时还应对相关人员进行培训使他们明确如何及何时使用这些预防/预警手段。

常言道“失败是成功之母”。应加强对以往发生的信息安全事件的总结和可能引发信息安全事件的有关信息的收集、分析判断和持续监测。

4．应急响应流程

应急响应流程是应急计划的核心精华部分，它描述并规定了信息安全事件发生后应采取的工作流程和相应条款，目的是保证应急响应能够有组织地执行，从而最大程度地保证应急响应的有效性。图 11.4 描述了整个信息安全应急响应流程。

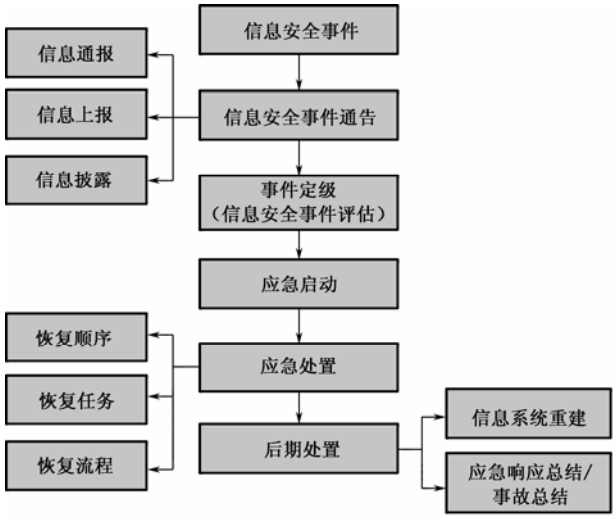


图 11.4　信息安全应急响应流程

整个应急响应流程中包含了信息安全事件通告、事件定级（信息安全事件评估）、应急启动、应急处置和后期处置 5 个部分，下面对这 5 部分分别进行阐述。

1）事件通告

事件通告部分又包括信息通报、信息上报和信息披露 3 部分。

Ⅰ．信息通报

信息通报是“横向”通报，分为**组织内**信息通报和**组织外**信息通报两部分。组织内信息通报的目的是在信息安全事件发生后迅速通知应急响应日常运行小组，并根据评估结果迅速通知所有相关人员，从而快速有序地启动和实施应急响应计划。组织外信息通

报目的是将相关信息及时通报给受到负面影响的外部机构、互联的单位系统及重要用户，同时根据应急响应的需要，应将相关信息准确通报给相关设备设施及服务提供商（包括电信、电力等）等外部组织，以获得适当的应急响应支持。值得注意的是，对外信息通报应符合组织对外信息发布的有关规定，避免出现由于轻率的信息发布而带来不必要的“心理恐慌”。

组织内信息通报是信息通报的重点和关键，因为它决定了组织处理安全事件的速度和效率，所以这里着重分析说明组织内信息通报。

在信息安全事件发生后，应通知应急响应日常运行小组或应急响应专家小组，确定事态的严重程度和下一步将要采取的行动。在损害评估完成后，要尽快通知应急响应领导小组。


可以通过各种方法完成事件通知，包括固定电话、移动电话等，其中手机短信群发方式由于简明、高效和避免重复通知等特点，受到众多应急响应通报平台的青睐。当然，应急计划制定者也要考虑在网络大规模阻塞的情况下其他的备选通报方案（如利用广电网进行电视通报等，但要考虑附带影响）。由于电子邮件无法确定能否及时阅读和有效回复，所以不建议通过电子邮件发送通知，除非是低等级、影响轻微的安全事件。

应急响应的通知策略应制定信息安全事件发生后某特定人员无法联络时的备选人选方案，并在应急响应计划中明确描述。一种通用通知方法是所谓的**呼叫树**。呼叫树应包括主要的和备用的联络方法，应确定在某个人无法联系上时应采取的规程。应急响应呼叫树示例如图 11.5 所示。

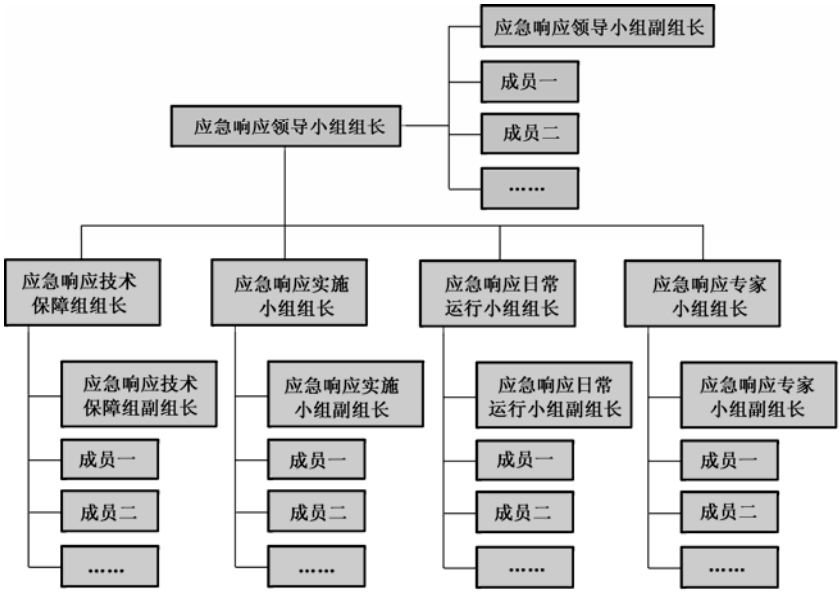


图 11.5　应急响应呼叫树示例

需要通知的人员应该在计划附件中的应急响应人员联络表中标明。应急响应人员联络表确定人员在其小组中的职位、姓名和联络信息（如家庭电话、工作电话、手机和家庭地址等）。应急响应人员联络表如表 11.1 所示。

表 11.1　应急响应人员联络表

小组名称	姓名	在小组中的职位	联络信息				
			工作电话	家庭电话	手机	电子邮件（备选）	家庭地址

Ⅱ. 信息上报

信息上报是“纵向”通报。信息安全事件发生后，应按照相关规定和要求，及时将情况上报上级主管或监管单位/部门。需要上报的信息安全事件一般属于 II 级和 II 以上的安全事件（见事件定级的介绍），对于低等级的安全事件可以予以记录存档，或以月报/季报/年报等形式提交给上级主管或监管部门，以供长期跟踪研究和大范围安全事态预报研究。安全事件报告表如表 11.2 所示。

表 11.2　安全事件报告表

信息安全事件报告表	
报告时间：年　月　日　时　分	
单位名称：	报告人：
联系电话：	通信地址：
传真：	电子邮件：
发生信息安全事件的信息系统名称及用途：	
负责部门：	负责人：
信息安全事件的简要描述（如以前出现过类似情况也应加以说明）：	
初步判定的事故原因：	
当前采取的措施：	

续表

信息安全事件报告表	
本次信息安全事件的初步影响状况：	
事件后果：	
影响范围：	严重程度：□　I 级　□　II 级　□　III 级　□　IV 级
值班电话：	传真：

III. 信息披露

信息发布的目的是避免信息安全事件影响被误传或讹传，及时掌握和引导公众舆论，同时规范组织内部人员的信息披露，保证信息发布口径的一致性。因此，信息安全事件发生后，应根据信息安全事件的严重程度，授权特定的小组（如政府部门的新闻发言人等）按照有关规定及时向新闻媒体发布相关信息，同时组织内的其他部门或者个人不得随意接受新闻媒体采访或对外发表自己的看法。



“5 • 12”汶川大地震发生后，陕西省地震局网站新闻曾被人篡改，并以该省地震局的名义发布了新的地震预报消息，造成了较大的负面影响。该局及时发现并处理了这起严重的信息安全事件，对虚假信息予以更正，平息了不必要的恐慌，有关责任人也受到了法律的制裁，参见第 12 章《法律和法规》。

2）事件定级

在本书前面所介绍的内容中，分类、分级的思想随处可见。因此对突发信息安全事件进行分类和分级，也是我们进行应急响应的必然选择。

确定信息安全事件发生后对系统损害性质和损害程度的评估，是启动和实施应急响应计划的前提。这个损害评估应该在确保人员安全（这里主要是指由于信息安全事件所带来的次生灾害，如医院信息系统安全事件导致 CT 机故障等）这个最优先任务的前提下尽快完成。所以应急响应日常运行小组或专家组应该是第一个得到事件通知的小组，以便尽快得出评估结论。损害评估的侧重点“因系统而异”，但是总的来讲应该从以下角度进行分析。

（1）受到紧急情况影响的业务系统或区域。无论在何种情况下，组织的业务连续性和重要性始终都是应急响应的首要目标。所以应当首先评估组织的主要业务系统或业务区域受到何种程度的影响，并以此作为事件定级的主要依据。

（2）潜在的附加影响或损失（即次生灾害）。由于信息系统将组织的业务与其他组

织的业务越来越密切地联系在一起，所以对安全事件的滞后影响、次生灾害也应当予以评估。

（3）造成紧急情况或系统中断的原因。在评估业务影响的同时，也应积极组织技术力量分析造成安全事件的原因。需要指出的是，对于许多组织而言，特别是那些业务连续性非常重要的组织，应当“先解决后问责”，如立即启动备份系统确保业务尽快恢复到正常状态，随后再分析事故起因（见 11.2.3 节中应急处置的介绍）。对于那些业务连续性要求不高的组织（如企业门户网站等），则可先分析事故起因，再按照应急响应计划（预案）确定解决办法。

（4）物理环境（如中心机房结构的完整性、电源、通信及制热、通风和空调的情况）的状况。要注意信息安全事件并不总是等于“黑客攻击事件”，在很多情况下是由于设备故障或物理环境改变甚至仅仅是通信线路接口松脱等引起的。所以在考虑事故定级的时候，也应快速检查物理环境是否有所改变。

（5）系统设备的总量和功能状态（如具备主要功能/具备部分功能/丧失所有功能等）。

（6）系统设备及其存货的损失类型（如水害、水灾或热能、物理及电涌影响）。

（7）被更换的项目（如硬件、软件、固件或支持材料）。

（8）估计恢复正常服务所需的时间。

完成损害评估后，应急响应日常运行小组应确定信息安全事件的类别与级别。表 11.3 是关于信息安全事件响应等级表，事件分类和定级需分别遵照《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986—2007），参考第 4 章信息安全事件分类和第 5 章信息安全事件分级，有兴趣的读者请具体参看《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986—2007）相关内容，这里不再赘述。

表 11.3　信息安全事件响应等级表

事件响应等级	内 容 描 述
I 级事件	现有的系统停机，或遭到严重攻击行为或安全事件，或对数据中心的业务运作有重大影响，持续时间小于 4h 的事件。持续时间超过 4h 则升级到重大责任事故
II 级事件	现有系统的操作性能严重降低，或由于网络性能失常或安全事件严重影响数据中心业务运作，持续时间小于 8h 的事件。持续时间超过 8h 则升级到 I 级事件
III 级事件	系统的操作性能受损，安全事件如病毒在小范围内发作，但大部分业务运作仍可正常工作，持续时间小于 8h 的事件。持续时间超过 8h 则升级到 II 级事件
IV 事件	在服务器、存储设备、安全设备等的功能、安装或配置方面需要信息咨询或技术支持。本级故障事件对数据中心的业务运作几乎无影响，或根本没有影响，持续时间小于 4h 的事件。持续时间超过 4h 则升级到III级事件

应急响应日常运行小组的人员应该通过经常性的应急演练等熟悉安全事件定级，因为事件的级别决定了应急响应的级别。一旦系统影响被确定，就应该将最新信息和对此情况的应急响应计划通知给应急响应领导小组。

Ⅳ级事件属于日常运行维护服务范畴，III级事件仍由日常运行维护服务人员处理，

但需要向应急响应有关人员告知；Ⅱ级事件和Ⅰ级事件属于应急响应事件，事件从Ⅳ级升级到Ⅲ级时，由运行维护服务人员及时通知应急响应小组启动应急响应计划。

3）*应急启动*

应急响应计划的启动（激活）代表“作战命令”的正式下达，组织的信息系统甚至整个组织就从“平时运行维护状态”转入了“战时应急状态”。计划的启动应注意以下 3 点。

（1）**启动原则：**果断、快速、有序；“果断”是指应急响应领导小组基于安全事件的评估结论，定下响应决心。因此事件评估是指挥决策的关键。“快速”与“有序”是指整个应急响应团队的协同要非常流畅，包括计划启动的通知、人员到位、事件处理、外协单位（如应急设备供应商等）进场等应按照响应流程有条不紊地展开。

（2）**启动依据：**一般而言，对于导致业务中断、系统宕机、网络瘫痪等突发/重大信息安全事件应立即启动应急响应计划。但由于组织规模、构成、性质等的不同，不同组织对突发/重大信息安全事件的定义可以不一样，因此，各组织的应急响应计划的激活条件可能各不相同。激活条件可以基于以下 4 方面考虑。

① 人员的安全和/或数据、设施的损失程度；

② 系统损失的程度（如物理的、运作的或成本的）；

③ 系统对于组织业务的影响程度（如保护资产的关键基础设施）；

④ 预期的中断持续时间等。

当对系统损害评估的结果显示一个或多个条件被满足时，就应该立即启动响应计划。

（3）**启动方法：**一般情况下总是由应急响应领导小组发布应急响应启动令。但需要提醒读者注意的是，在特殊情况下（如特别重大信息安全事件的发生或特殊组织、特殊岗位等），事件发生现场人员应按照预先制定的响应方案立即采取抢险措施，同时请示应急响应领导小组发布应急响应启动令，以获取更大范围的支持。一种有效的方法是由应急响应领导小组事先授权给特殊岗位的人员，以便在特殊情况下第一线人员能够果断决定。但使用这种“例外”的方式要慎重，在平时就应该由应急响应领导小组进行仔细研究和审批。

4）*应急处置*

应急响应启动令一旦下达，就应立即采取相关措施抑制和清除信息安全事件影响，避免造成更大损失。读者可能已经注意到我们使用了“抑制”和“清除”这两个近义词。事实上它隐含了信息安全应急响应工作中两个相关的概念，需要与读者进一步探讨。一个是



1996 年，美国克林顿总统发布了保护国家基础设施的总统令。该总统令主要基于美国政府智囊机构兰德公司 1995 年提交的一份研究报告。兰德公司通过模拟一场针对美国重要基础设施信息系统的网络攻击而带来的灾难，向美国联邦政府决策层展现了这些基础设施信息系统的极端重要性和脆弱性。2002 年，布什政府进一步强化了基础设施的保护要求。

“应急响应”，一个是“灾难恢复”。目前在信息安全领域对这两个概念没有进行严格的区分，因为这牵涉到组织的规模、安全事件的影响范围等因素。一般而言，如果一个组织的规模越小、业务范围越窄、受影响的系统越少，应急响应与灾难恢复就属于同一个范畴。但对于关键部门、重要信息系统（如省级或省级以上的电子政务系统、金融、电力、能源、交通、航空等国家重要基础设施的信息系统），应急响应与灾难恢复就应当加以区别，这就如同特大自然灾害发生后的“救灾抢险”与“灾后恢复”就是两个不同（当然也是密切相关）的阶段，各自有其工作重心、恢复时间和恢复目标。有兴趣的读者应当参阅国家有关《信息系统灾难恢复指南》等标准和国外有关机构的相关资料，以便在应急响应和灾难恢复工作中加以细化。考虑到本书的篇幅和主要读者群及中国目前信息化的发展水平等因素，这里暂时将应急响应和灾难恢复等同对待，同时在“后期处置”中对灾难恢复做一个简要介绍，特此说明。

在采取应急措施有效控制了信息安全事件影响后，就应开始恢复操作，恢复阶段的行动集中于建立组织的临时业务处理能力（如备份数据的导入等）、修复受损害的系统、在原系统或新设施中恢复业务运行能力等应急措施。

目前国家有关标准中的应急处置规定主要对恢复顺序和恢复任务做出了一些规范性要求，至于具体如何处置特定的信息安全事件（如拒绝服务攻击、恶意代码攻击等）没有做出规定，这就需要相关人员参考其他标准（如《计算机安全事件处理指南》NIST SP800-61 等）并结合自身工作的特点加以细化，我们也将在本章的案例分析中抛砖引玉，供读者批判吸收。

下面分别对恢复顺序、恢复任务和恢复流程进行说明。

Ⅰ. 恢复顺序

在进行系统应急恢复时，恢复顺序就是 BIA 中确定的系统优先顺序。恢复的顺序应该反映出系统允许的（也往往称为可以容忍的）中断时间。要注意这里的中断时间不仅是指受损设备本身，还应该由设备受损后给组织业务造成的影响来决定。例如，需要事先确定主要数据库服务器、核心交换机等关键设备受损后，对整个组织业务影响可以容忍的中断时间是多少，以避免对相关系统及其业务应用造成进一步重大影响。容忍时间越短的，恢复优先级越高，这就好比抢救一名心力衰竭并且肢体也受到严重创伤的病员，首先就要实施电击起搏、止血等抢救，然后再进行受创肢体的消毒、包扎等工作。

Ⅱ. 恢复任务

为了有条不紊地进行恢复操作，应急响应计划需要提供详细的恢复任务，并事先将这些任务分配给适当的恢复小组。恢复任务通常涉及以下行动。

（1）获得访问受损设施和/或地理区域的授权。例如，在应急响应人员抵达现场时，由于受损设施在平时往往有相应的安全防护手段（口令等），或者涉及组织敏感业务而需要授权进入/使用，因此要保证必要的信息沟通以便抢险人员“无障碍”地开展工作。对于进行远程网上救援指导的专家，这些信息沟通就显得更为重要。

（2）通知相关系统的内部和外部业务伙伴。内部人员和外部业务伙伴除了参与应急响应的人员之外，还要包括组织的业务部门相关人员。例如，一个组织的财务软件系统严重受损，原材料采购部门和销售部门的人员就应获得通知，同时外部业务伙伴如银行等相关人员也应获得通知。

（3）获得所需的应急用品和工作场所。应急用品包括软件（如操作系统、数据库、数据恢复软件、组织业务系统所运行的大型专用软件等）、硬件（如替换双机热备中受损主系统的硬件、数据恢复专用设备、存储设备/介质和光缆等）和网络检测设备等；应急工作场所一般情况下应当是在事故发生现场，但对于重大安全事件，如机房失火后七氯丙烷大量溢出等情况，则需要开辟临时工作场所。这些工作均需要根据组织的实际情况，事先考虑在应急计划之中。

Ⅲ. 恢复流程

针对上述恢复任务，需要整理出分解给各个应急小组的恢复流程。应急响应计划的编写人员要将其逐一细化并落实在应急响应计划中。恢复流程应按照直接和分步骤的方式书写。为了防止在信息安全事件中产生误解或混乱，不能假定或忽略规程的步骤，并且需要在应急演练中不断完善。

检查列表（check list）是在制定恢复流程中常使用的一种简便方法，它有助于细化恢复流程，查找问题结点。表 11.4 是一个数据库应急恢复任务小组的恢复流程检查表，供读者参考并举一反三。

表 11.4　数据库恢复流程检查表

任 务 名 称	××信息系统数据库应急恢复小组
任务目标及内容	用于从备份磁带中恢复一个文件。恢复小组负责所有关键文件的重新装载
恢 复 流 程	操 作 指 南
第一步	确定将要进行恢复的文件及其日期
第二步	使用磁带记录本确定磁带编号
第三步	如果磁带不在磁带库中，则要求×××部门提供磁带
第四步	收到磁带时，将日期和时间填入日志
第五步	将磁带放入驱动器中并开始数据恢复
第六步	当文件恢复完毕时，通知数据库应急恢复小组的负责人
第七步	填写事故恢复/安全事件报告单

5）后期处置

通过应急处置成功解决信息安全事件后，应急响应工作并未结束，还需要尽快组织相关人员进行信息系统重建，同时还需要对信息安全事件应急响应进行总结，如果有必要还需对应急响应计划进行完善。

Ⅰ. 信息系统重建

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。具体的方法是：

（1）统计分析各种数据，查明原因。例如，收集和分析各种日志记录和监控设备录像等。这一个步骤在事后的责任追究甚至法律介入时将起到非常关键的作用。组织应指定专人（或专业机构）妥善保管各种电子文档。

（2）对信息安全事件造成的损失和影响及恢复重建工作进行分析评估。对照 BIA 所确定的各项指标，评估现有的状态及与这些指标之间的差距，进而分析弥补这些差距所需要投入的各种资源（人力、物力、重建周期等）。

（3）认真制定恢复重建计划。在充分分析论证的基础上，制定重建计划并组织实施信息系统重建工作。对已经发生的安全事件要有足够的应对措施。

（4）重建工作完成后，对所采取的措施要进行（简要的）风险评估，使得组织的业务从“战时状态”恢复到“平时状态”，并为下一次又进入“战时状态”做好准备（所以说风险评估与应急响应是一个组织信息安全的常态性工作）。

Ⅱ. 应急响应/事件总结

应急响应/事故总结是应急处置之后应进行的工作，具体工作包括：

（1）分析和总结事件发生原因；

（2）分析和总结事件现象；

（3）评估系统的损害程度；

（4）评估事件导致的损失；

（5）分析和总结应急处置记录；

（6）评审应急响应措施的效果和效率，并提出改进建议；

（7）评审应急响应计划的效果和效率，并提出改进建议。

这部分工作也可以与“信息系统重建”结合在一起。表 11.5 提供了一个信息安全事件应急响应总结的模板。

表 11.5　信息安全事件应急响应总结报告模板

信息安全事件应急响应结果报告表	
原事件报告时间：　　年　月　日　时　分	
备案编号：　　年　月　日　第　号　总第　号	
单位名称：	联系人：
联系电话：	通信地址：
信息系统名称及用途：	
已采用的安全措施：	
信息安全事件的补充描述及最后判定的事件原因：	
本次信息安全事件的初步影响状况：	
事件后果：	影响范围：

续表

信息安全事件应急响应结果报告表
严重程度： ☐ I 级事件　☐ II 级事件　☐ III 级事件　☐ IV 事件
本次信息安全事件的主要处理过程及结果：
针对此类信息安全事件应采取的信息系统安全保障措施和建议：
报告人签名：

5．应急响应保障措施

“兵马未动，粮草先行”。应急响应计划作为一个组织的“战时”方案，后勤保障是取胜的前提条件。考虑到各个组织的性质和需求可能存在很大的差异，本书中描述的具体内容是可选择的，也可以做适当调整，但人员保障、物质保障和技术保障这 3 个大的方面是应急计划必须包括的内容。

1）人员保障

在整个信息安全的应急响应过程中，人员保障是最重要的，任何与应急响应有关的工作都需要根据角色分工直接落实到人，而不仅是层层传达到各级部门。人员保障分为管理和技术两个方面。

Ⅰ．管理人员保障

组织要依据自身的职责制定具体角色和职责分工细则，细则需要制度化，并依据现有人员的实际情况制定合理工作安排，工作安排要直接落实到人，形成所有管理人员独立的应急操作手册，如有人员工作安排变动时要及时更正手册，并保证管理人员所使用的手册版本是最新的。管理人员的具体保障由应急响应领导小组统一规划和组织管理。

Ⅱ．技术人员保障

技术人员保障通过建立应急响应技术保障小组和应急响应专家小组来进行，所有技术保障问题统一由应急响应技术保障小组负责。应急响应技术保障小组要依据应急的技术需要制定具体角色和职责分工细则。细则需要制度化，并依据现有人员的实际情况制定合理工作安排。工作安排要直接落实到人，形成所有技术人员独立的操作手册，如有人员工作安排变动时要及时更正手册，并保证技术人员所使用的手册版本是最新的。



北美的加拿大以枫叶之国闻名于世，然而在漫漫的冬季大雪纷飞之时，所有道路都铺满了积雪。不少“上班族”都与铲雪公司签署了合同，以保证他们在大雪季节能够准时出行上班。但往往让人哭笑不得的是，小雪的时候人们可以“自扫门前雪”，而大雪的时候，家家都需要铲雪公司第一时间来服务……

由于应急响应技术保障小组除了建立自身的技术支持队伍外，所确定的角色与职责大多需要依赖合作者（包括社会力量和专家等），如各种型号的设备

或专用软件等，均需要集成商、供货商或开发商技术支持部门的配合。因此，应急响应技术保障小组要建立完备的技术培训机构和操作管理方案，保证新技术与应急响应技术的及时培训，保证应急响应技术的有效性。

应急响应技术保障小组可以依据自身的工作特点、协作单位与人员的具体情况制定应急响应协同调度方案，但无论采取什么方案均要有具体的协同工作记录以备审计。这里需要特别指出的是，由于设备供货商或研发单位的技术支持部门可能同时与多家组织签署了服务合同，所以要明确规定大规模应急事件发生的时候，这些第三方协作机构的服务出勤率。而第三方协作机构也要根据自身的实际情况，对自身的技术支持队伍和服务对象的重要性进行优先级排序，避免多起安全事件并发的时候产生混乱。

2）物质保障

物质保障是实现应急响应的基础条件，包括基础物质保障和应急响应物质保障。

Ⅰ. 基础物质保障

应分析为了及时启动信息安全事件应急响应流程，需要什么样的基础物质保障，即基础物质需求分析，这些需求应与技术保障和日常管理相关联，即应保证日常技术保障的实现、日常管理工作的开展和应急响应技术服务在应急处理时的及时到位。物质需求由应急响应技术保障小组提出，应急响应日常运行小组负责落实。

Ⅱ. 应急响应物质保障

应急响应物质保障包括财力保障、交通运输保障、治安维护和通信保障等部分。

（1）财力保障，要保证所需信息安全事件应急响应资金。这部分内容既包括应急设备采购、组织内部人员所需的必要费用，也包括应急响应外协单位的服务费用。

（2）交通运输保障，要协调保证紧急情况下应急交通工具的优先安排、优先调度、优先放行，确保运输安全畅通；要依法建立紧急情况社会交通运输工具的征用程序，确保抢险救灾物资和人员能够及时、安全送达。

根据应急处置需要，对现场及相关通道实行交通管制，开设应急响应“绿色通道”，保证应急救援工作的顺利开展。

（3）治安维护，重大信息安全事件发生后，特别是影响范围已经超出了信息系统或组织内部本身的情况下，治安维护工作除了通常意义下的维持应急抢修秩序，还包括对事发现场的保护，以利于事故原因取证。

（4）通信保障，对于国家和区域性行政部门，或者大型基础设施信息系统（电力、航空、交通、能源和金融等），应建立健全应急通信、应急广播电视保障工作体系，完善公用通信网，建立有线和无线相结合、基础电信网络与机动通信系统相配套的应急通信系统，确保通信畅通。对于规模较小的组织，尽管所依赖的基础通信设施未受到影响，但也应有通信保障预案，确保多渠道信息通报机制的畅通（见 11.2.3 节中信息通报相关内容）。

3）技术保障

技术保障是信息安全事件应急响应的必备手段，由应急响应技术保障小组统一负责，它包括应急响应技术服务与日常技术保障两部分。

Ⅰ．应急响应技术服务

根据对组织 BIA 的分析，应急响应技术保障小组可制定信息安全事件技术应对表，并以此来选择合适的技术服务者或服务机构，同时要明确组织与个人、组织与服务机构的职责和沟通方式。

Ⅱ．日常技术保障

日常技术保障包括事件监控与预警的技术保障、应急技术储备两部分。

（1）事件监控与预警的技术保障。本书前面曾经指出，预防是应对安全突发事件“成效比”最高的方式之一。而预防则取决与日常工作中对各种“蛛丝马迹”的发现和分析，即事件监控与预警。事件监控与预警的技术保障由应急响应日常运行小组负责，是应急响应日常运行小组的常规职责。有条件的组织在建立相应的监控与预警部门之后，需要由该部门落实具体的监控与预警措施，并与应急响应日常运行小组保持随时的信息交流（如果这个部门不是应急响应的日常运行小组的话）。信息系统的复杂性、虚拟性和海量信息处理的时效性等均加大了对事件监控和预警的难度，所以组织也应有针对性地使用各种网络监控工具和分析工具，如本书 8.2.2 节所介绍的 Sniffer、逆火等常用工具，逐步加强对事件的监控与预警能力。对信息安全事件进行日常监控的方法（手段）、流程、记录等应明确是谁的职责，落实到人。

（2）应急技术储备。应急技术储备由应急响应技术保障小组配合应急处理技术服务和技术人员保障来实现。尽管对于不同规模的组织，应急技术储备的广度和深度均各不相同，但包括“数据恢复技术”等技术储备是所有组织均需要的。建议组织根据应急技术服务表来确定和不断完善应急技术储备方案，从而做到“招之即来、来之能战、战之能胜”。当然，这个原则对人员、物力等保障也是适用的。

6．附件

有关附件的内容参见 11.3.2 节的“南洋烽火计划”。

11.2.4　应急响应计划的培训、演练和更新

如果应急计划不经过培训和演练，那么应急计划就仅仅是“应付计划”。一旦重大信息安全事件真的来临，除了给组织带来巨大损失之外，这种应付计划也将成为组织的耻辱和笑柄。因此一个组织，特别是应急响应领导小组要高度重视对相关应急响应人员的应急计划的培训和演练。

1．计划的培训

应急响应计划的培训是应急响应人员必须接受的技能训练之一（另外一个是计划的

演练，见下一条）。培训必须定期举办。我们反复强调过“应急响应就是和灾害的蔓延争速度、抢时间”，所以培训的组织者要让培训人员达到对计划“了然于胸”的水平，使得应急响应人员能够无须实际文档的协助就能够执行相应的恢复规程。这在信息安全事件造成影响的最初几个小时里，由于系统宕机甚至机房失火等原因而无法获得书面**或电子版本的应急响应计划的情况下，具有非常重要的意义。**

2．计划的演练

计划的演练如同军事演习，是“平时状态”下论证应急响应计划有效性最好的方法。演练能发现和解决计划的缺陷，还能评估应急人员快速有效实施应急响应计划的能力。每一个信息安全应急响应计划的细节和操作流程都应该得到演练，以确保各小组之间的协同能力、人员操作的准确性和计划整体的有效性。

计划的演练包括制定演练计划、组织演练和计划更新（演练总结）等几个环节。

（1）演练计划。实际上就如同军事领域中的演习计划一样，要明确此次演练的目标、所演练的主要内容、演练成功/失败的评价指标、演练人员的组成、演练的各种方案（如同电影导游一样设计各种演练场景）、演练所需的各种支持条件等。需要指出的是，演练计划的制定者要充分考虑演练计划的成本、参演人员的积极性及尽量少地干扰组织的正常业务。因此，既要考虑全系统的演练方案，也要制定分系统的演练方案。演练计划由应急响应技术保障小组或应急响应专家组负责撰写。



2005 年，由中日韩三国牵头组织了亚太联合网络安全应急演练，演习预案是：一个假设的跨地区大规模僵尸网络对韩国发动针对多个重要网站的攻击。

在演练中，亚太网络安全应急联盟（APCERT）在接到韩国 CERT 的报警后，APCERT 各成员在各自国家和地区迅速采取措施阻止并摧毁了该僵尸网络。

参加这次演练的有 10 个 APCERT 成员，分别来自澳大利亚、中国、中国香港、中国台湾、日本、韩国、马来西亚、菲律宾、新加坡 9 个经济体。

这次演练旨在检验各成员应急响应和协作配合的能力。APCERT 主席格莱姆•茵格莱姆说，演练结果表明，APCERT 成员能够通过发挥各自经济体的作用，来积极协助其他成员处理涉及本经济体的网络攻击事件。

（2）演练组织。演练分为“图上推演”和“实兵演练”两种基本方式。

图上推演：如同军事演习中的“沙盘演习”。尽管这种方式有点给人“纸上谈兵”的滑稽感觉，但却是保持应急响应计划处于良好状态并且演练成本较低的方式。

图上推演的参与者并不进行实际的操作，而是根据演练计划和自己担负的角色进行“动口不动手”的推演。图上推演也是进行应急响应计划培训的有效方法之一。

实兵演练：实兵演练是仅次于真实事件发生的练兵方式。首先要提醒读者注意的是，这种演练成本较高，在演练开始之前，要进行各种应急准备（如数据的备份工作等），以免自己将自己“弄假成真”，带来不必要的损失。由于实兵演练毕

竟是可以自行控制的“安全事件”，而且仅有培训和图上推演，应急响应人员得不到充分的锻炼，应急计划也得不到全面的论证，所以实兵演练也是必须的。

实兵演练可以按照预设情况由组织的内部人员进行演练，也可以采用“背靠背”的方式，邀请其他专业机构和技术部门的人员与组织的应急响应人员进行对抗演练，这种“背靠背”的对抗演练对于大型组织，如国家基础设施信息系统应急响应能力的提高尤为重要，即使成本较高，也应有序、适时地组织演练。

（3）计划更新。由于业务战略的转移、技术的更新或组织内外政策变化等因素会造成信息系统的频繁变化，如一个城市的社会保障信息系统以往只是承担失业统计、就业指导及相关救助金额的发放等方面的职责。近年来根据国家政策要求又增添了医疗保障的管理职责，而无论是社会保险还是医疗保险，均属于社会民生的大事，信息系统一旦崩溃，将带来严重的社会影响（信息安全事件带来重大公共安全事件）。因此，原有的社保信息系统应急计划就必须进行相应的调整，如原有的应急外协单位就从银行延伸到医院…… 由此可见，应急响应计划的定期检查和更新是至关重要的，应确保新的应急需求、响应流程等能够被添加进来，陈旧的响应模式、技术、对象等能够及时被清除。计划中应该至少每年进行一次针对正确性和完整性的检查，在计划的任何部分发生重大变化时也应该进行更新，这是一项基本的要求。某些部分应该得到更频繁的检查，如联络清单（呼叫树）等。根据信息系统类型和重要程度的不同，对计划内容和规程的评估可能会更加频繁。

一种对计划进行检查常用的方式是将计划的演练与计划检查（更新）结合起来。演练的结果和学习到的经验教训应该记录到文档中。在演练中收集到的各种有助于提高应急响应计划效率的信息应该添加到应急响应计划中。

在进入案例分析之前，最后介绍一下应急计划文档保管的要求。

11.2.5　文档的保存、分发与维护

尽管要求应急响应人员对应急计划“了然于胸”，但作为一个组织管理质量体系的体现，需要以对待组织最重要的文件的态度对待应急响应计划，并对其进行有效管理。经过审核和批准的应急响应计划文档应当按照以下方式进行管理。

（1）由专人负责保存与分发；

（2）复制多份并在不同的地点保存；

（3）分发给参与应急响应工作的所有人员；

（4）在每次修订后对所有复制件统一更新，并保留一套，以备查阅；

（5）旧版本应按有关规定销毁。

为了保证应急响应计划的有效性，应从以下 3 方面对应急响应计划文档进行严格的维护。

（1）业务流程的变化、信息系统的变更、人员的变更都应在应急响应计划文档中及

时反映。

（2）应急响应计划在培训、演练和信息安全事件发生后实际执行时，其过程均应有详细记录，并应对培训、演练和执行的效果进行评估，同时对应急响应计划文档进行相应的修订。

（3）应急响应计划文档应定期评审和修订，至少每年一次。

计划、策略和政策的变化应该由应急响应日常运行小组进行协调，如果需要，应急响应日常运行小组应该与组织的日常工作计划安排者或项目相关的代表就变化情况进行沟通。应急响应日常运行小组应该使用变化记录对计划更改进行记录，变化记录包含页码、变化备注和变化日期。应急计划文档变更记录如表 11.6 所示。

表 11.6　应急计划文档变更记录

变 化 记 录			
页　码	变 化 备 注	变 化 日 期	签　名

11.3　应急响应计划案例分析

作为本章的结束，将给出本书第三个，也是最后一个案例分析。考虑到本书主要读者群的背景，我们选择了大学校园网作为制定应急响应计划的剖析对象。尽管如此，其中所蕴涵的基本思想也适用于其他信息系统的应急响应情况。

11.3.1　南海大学信息安全应急响应计划示例

南海大学在校师生员工 5 万余人，分设 A、B、C、D 四个校区。是中国东南沿海地区最主要的“211”和“985”高校之一。近年来学校为了提高办学质量，建成了国内一流的“数字化校园——嘉庚网”。“嘉庚网”与 Internet 相连。作为服务于教育、科研和行政管理的计算机网络，“嘉庚网”实现了四个校区、各二级学院、“嘉庚数字图书馆”、行政部门内部网络的互联互通。

随着校内、外用户的快速增长，“嘉庚网”已经成为南海大学各项教学科研工作不可或缺的基础设施，一旦发生重大信息安全事件，对学校工作的正常有序开展将造成极大的破坏。因此，制定和检验“嘉庚网”应急响应计划——“南洋烽火计划”非常必要和迫切。

11.3.2　“南洋烽火计划”

1．总则

1）编制目的

为了切实做好南海大学信息安全事件的防范和应急响应工作，进一步提高学校预防和控制信息安全事件的能力和水平，减轻或消除信息安全事件的危害和影响，确保“嘉庚网”信息安全，结合学校工作实际，特制定“南洋烽火”应急响应计划，请各有关单位遵照执行。

2）编制依据

为了贯彻落实《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《计算机信息网络国际联网管理暂行规定》等国家有关法律、法规及学校制定的《“嘉庚网”公共信息管理暂行办法》、《“嘉庚网”信息保密管理办法》等文件精神，依据《信息技术 安全技术 信息安全事件管理指南》（GB/Z 20985—2007）、《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986—2007）、《信息安全技术 信息系统灾难恢复规范》（GB/T 20988—2007）等国家有关标准，并参照《信息安全技术 信息安全应急响应计划规范》（草案），制定“南洋烽火计划”。

3）适用范围

本计划适用于：

（1）“嘉庚网”运行及网络信息方面发生的有可能影响学校、社会和国家安全稳定的紧急事件；

（2）由于其他重大事件的发生影响到“嘉庚网”正常运行或网络信息安全，并由此可能影响到学校、社会和国家安全稳定的事件。

本计划包括“嘉庚网”及网上的各种信息服务等。

4）工作原则

以人为本，预防为主；统一领导，分级负责；依法规范，加强管理；快速反应，协同应对；依靠科技，资源整合。

2．角色及职责

1）角色的划分及职责

“南洋烽火”应急响应工作机构按角色划分为四个功能小组：应急响应领导小组，应急响应实施小组，应急响应日常运行小组和应急响应专家小组。信息安全事件发生后，在应急响应领导小组的统一部署下，工作人员各施其职，并严格按照本计划组织实施应急响应工作。

（1）应急响应领导小组：由学校分管“嘉庚网”建设的常务副校长任组长、学校网络信息中心主任任副组长，成员单位包括党办、校办、网络信息中心、保卫处等。领导小组负责领导和决策信息安全应急响应的重大事宜。主要包括制定工作方案，提供人员

和物质保证，审核批准应急响应策略，审核批准本计划，批准和监督本计划的执行，指导应急响应实施小组的应急处置工作，启动定期评审、组织应急演练、修订本计划及负责本计划的外部协作。

（2）应急响应实施小组：由网络信息中心牵头，通信学院、计算机学院、软件学院等相关二级学院协同组成。当由于系统崩溃、病毒攻击、非法入侵等原因造成“嘉庚网”运行异常或瘫痪时，根据信息安全事件的发展态势和实际控制需要，具体负责现场应急处置工作，尽快恢复“嘉庚网”的正常运行。

（3）应急响应日常运行小组：由网络信息中心承担。负责做好“嘉庚网”信息安全的日常巡查及其日志保存工作，以确保网络异常的早期预警。同时负责信息安全事件发生后的损失控制和损害评估，并协助应急响应实施小组实施应急响应工作。

（4）应急响应专家小组：委托南海市信息安全技术中心负责组建，成员包括南海市信息安全技术中心和“巨浪”数据恢复技术中心等 4 名专家。应急响应专家组负责在 I、II 级安全事件发生时，配合应急响应实施小组评估灾害情况，查明事故原因，协助网络信息中心进行早期预警分析，指导应急演练，向应急响应领导小组建议本计划的更新等工作。

应急响应工作机构具体设置见附件 A。

2）外部协作

依据“嘉庚网”信息安全事件的影响程度，如需向上级部门及时通报准确情况或向其他单位寻求支持时，应与相关管理部门及外部组织机构保持联络和协作，主要包括以下 3 个方面。

（1）管理部门：南海市政府公共突发事件应急响应办公室、市信息化领导小组办公室、南海市公安局公共网络安全监察支队、南海省公安厅公共网络安全监察总队、国家计算机网络应急技术处理协调中心（CNCERT/CC）南海地区分中心、中国教育科研网（CERNET）华南地区分中心、中国电信南海分公司网管中心等。

（2）外协厂商：华为公司南海分公司、CISCO 公司华南地区分公司、IBM 公司华南地区分公司、联想公司华南地区分公司、有关信息安全产品供货商驻南海办事处、红旗 Linux 公司南海分公司、微软大中华区华南地区分公司、永中 Office 公司南海办事处、“蔚蓝”软件公司（“嘉庚网”大型应用软件开发商）华南地区办事处等。

（3）外协机构：南海市信息安全技术中心、“巨浪”数据恢复技术中心等。

3．预防和预警机制

1）信息监测及报告

建立与完善信息安全事件检测、预测制度。按照“早发现、早报告、早处置”的原则，网络信息中心应加强对信息安全事件和可能引发信息安全事件的有关信息的收集、分析判断和持续监测。

如发现有异常情况或有信息安全事件发生时，网络信息中心要及时进行初步处理并

立即向应急响应领导小组报告。

2）预警

网络信息中心接到信息安全事件报告后，经初步核实，将有关情况及时向应急响应领导小组报告，并会同应急响应专家组进一步进行情况综合，研究分析可能造成损害的程度，提出初步行动对策。应急响应领导小组视情况召集协调会，决策行动方案，发布指示和命令。

3）预防机制

网络信息中心要加强对“嘉庚网”安全的防护工作和应急处置准备工作的监督检查，提高防范网络攻击、病毒入侵、网络窃密等的能力，防止有害信息传播，保障“嘉庚网”的安全畅通。

同时网络信息中心应密切关注国家相关部门或国际权威组织发布的病毒预防警报，及时获取病毒的名称、种类和传播方式等有关信息，有效地防止计算机病毒的入侵。

4．应急响应流程

1）事件通告

（1）信息通报。学校各单位在信息安全事件发生后，立即通知网络信息中心使其能够确定事态的严重程度和下一步将要采取的行动。在损害评估完成后，通知应急响应领导小组。应急响应领导小组在决定启动应急响应后通知所有小组的负责人，并将事件的细节通知他们。收到应急响应领导小组的通知后，小组负责人应及时通知各自小组成员，并将所有适当信息通知小组成员，小组成员应做好应急响应和重新配置的准备工作。

需要通知的人员清单详见附件 B。

（2）信息上报。对于重大的校园信息安全事件，由应急响应领导小组报上级主管部门（见外协单位－管理部门名单），请求上级部门帮助指导。

上报表格详见附件 C。

（3）信息披露。根据信息安全事件的严重程度，应急响应领导小组指派有关人员按照学校相关规定和要求及时向新闻媒体发布相关信息，同时其他小组和个人必须坚守各自岗位，未经允许，不得擅自发布误导信息，共同做好维护稳定工作。

2）事件分类与定级

信息安全事件发生后，网络中心对事件进行评估，确定事件的类别与级别。

（1）事件的分类。“嘉庚网”信息安全事件可分为 5 类：

① “嘉庚网”内网网站主页被恶意篡改、交互式栏目（如校园 BBS 论坛）里发表反政府、分裂国家、不利于民族团结、色情等内容的信息，以及损害国家、学校所在地区和学校声誉等方面的谣言。

② “嘉庚网”内网网络应用服务器被非法入侵，应用服务器上的数据被非法复制、修改和删除。

③ “嘉庚网”内网有关学校科研、教学及学校行政管理有关的敏感数据被泄露或未经授权被访问。

④ 在“嘉庚网”外网网站上发布的内容违反国家的法律、法规或侵犯知识产权，已经造成严重后果。

⑤ 病毒的大规模爆发和网络攻击。

（2）事件的定级。“嘉庚网”信息安全事件分为 4 级：一般（Ⅳ级）、较大（Ⅲ级）、重大（Ⅱ级）和特别重大（Ⅰ级），对应颜色依次为蓝色、黄色、橙色和红色。

蓝色事件（Ⅳ级）：“嘉庚网”上出现的非法信息，在校内造成一定影响，但尚未在社会上造成影响；由于病毒攻击、非法入侵等原因，200 台以内的用户主机不能正常工作。

蓝色事件在 24h 之内无法解决，则自动升级为黄色事件，并启动黄色事件响应程序。

黄色事件（Ⅲ级）：“嘉庚网”上出现的非法信息，在校内造成广泛影响，并在社会上造成一定的影响；由于病毒攻击、非法入侵等原因，致使学校部分校区出现网络瘫痪，或者 FTP 及部分网站服务器不能响应用户请求。

黄色事件在 8h 之内无法解决，则自动升级为橙色事件，并启动橙色事件响应程序。

橙色事件（Ⅱ级）：“嘉庚网”上出现的非法信息，在校内造成实质性影响，并在社会上造成严重影响；由于病毒攻击、非法入侵等原因，致使学校大部分校区网络瘫痪，或者邮件、“校园一卡通”计费服务器不能正常工作。

橙色事件在 8h 之内无法解决，则自动升级为红色事件，并启动红色事件响应程序。

红色事件（Ⅰ级）：“嘉庚网”上出现的非法信息在校内外造成重大实质性影响，并严重危害国家和社会；由于病毒攻击、非法入侵等原因，致使“嘉庚网”整体瘫痪，或者学校网络中心全部 DNS、主 Web 服务器不能正常工作；由于病毒攻击、非法入侵、人为破坏或不可抗力等原因，造成“嘉庚网”与 Internet 的连接中断。

红色事件在 4h 之内无法解决，则成为重大信息安全责任事故，需按照学校有关规定上报上级有关部门（见本节“外部协作”所罗列的管理部门名单）。

3）*应急启动*

对于红色（Ⅰ级）和橙色（Ⅱ级）事件应按照快速有序的原则启动本计划，并由应急响应领导小组发布应急响应启动令。

对于黄色（Ⅲ级）和蓝色（Ⅳ级）事件，通过日常监测和维护就可以解决的安全事件则不需启动本计划。

4）*应急处置*

本计划启动后，应急响应实施小组应立即采取相关措施抑制信息安全事件的影响，避免造成更大损失。具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的 IP 地址或其他网络用户信息，修复被破坏的信息，恢复网络信息系统。

按照信息安全事件的性质分别采用以下方案。

（1）病毒传播：针对这种现象，要及时断开传播源，判断病毒的性质、采用的端口，然后关闭相应的端口，在网上公布病毒攻击信息及防御方法。

（2）入侵：对于网络入侵，首先要判断入侵的来源，区分入侵来自于 Internet 还是“嘉庚网”内部。入侵来自 Internet 的，力争定位和取证入侵的 IP 地址，及时关闭入侵的端口，限制入侵 IP 地址的访问，在无法制止的情况下可以采用断开网络连接的方法；入侵来自“嘉庚网”内部的，查清入侵来源，如 IP 地址、上网账号等信息，同时断开对应的交换机端口并进行取证，然后针对入侵方法部进行署或更新入侵检测设备。

（3）信息被篡改：这种情况一旦被发现，要求马上断开相应的信息上网链接，并尽快恢复被篡改信息。

（4）网络故障：一旦发现，可根据相应工作流程尽快排除。

（5）其他没有列出的不确定因素造成的灾害，可根据总的安全原则，结合具体情况，做出相应的处理。不能处理的可以请示相关的专业人员。

5）后期处置

通过应急处置成功处理信息安全事件后，应急响应工作并未结束，还需要尽快组织相关人员进行网络信息系统重建或调整，同时还需要对信息安全事件应急响应工作进行总结。

（1）信息系统重建。在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。

网络信息中心负责统计各种数据，查明原因，会同应急响应专家组或外协单位对安全事件造成的损失和影响及恢复重建能力进行分析评估，认真制定恢复重建计划，迅速组织实施信息系统重建，并在改建完成后进行风险评估。

（2）应急响应工作总结。回顾并整理发生信息安全事件的各种相关信息，尽可能地把所有情况记录到文档中。发生重大信息安全事件时，应急响应实施小组应当在事件处理完毕后一个工作日内将处理结果报网络信息中心备案。通过对信息安全事件进行统计、汇总及任务完成情况进行总结和汇报，不断改进信息安全应急响应计划。

“重大信息安全事件应急响应结果报告表”见附件 D。

5．应急响应保障措施

按照职责分工和应急响应计划，切实做好应对信息安全事件的人力、物质、技术等保障工作，保证应急响应工作和恢复重建工作的顺利进行。

1）人力保障

加强学校信息安全人才培养，强化信息安全宣传教育，建设一支高素质、高技术的信息安全核心人才和管理队伍，提高信息安全防御意识。此项工作由网络信息中心牵头，通信学院、计算机学院和软件学院会同完成。

2）物质保障

学校要根据近几年全国甚至全世界网络信息系统安全防治工作所需经费情况，将本

年度信息安全应急响应经费纳入年度财政计划和预算，建立专项资金用于“嘉庚网”安全事件的处置，提前购买相应的应急设施，避免时间拖延造成不必要的损失，保证应急响应队伍技术装备的及时更新，以确保应急响应工作的顺利进行。

3）技术保障

加强网络信息中心的建设与发展，建立预警与应急处理的技术平台，进一步提高信息安全事件的发现和分析能力。从技术上逐步实现发现、预警、处置和通报等多个环节和不同的网络、系统、部门之间应急处理的联动机制。

6．计划的培训和演练

为强化学校有关应急响应人员对“南海烽火计划”的熟悉程度，应急响应领导小组应在 7 月学校放假后的第一个星期一，组织有关部门人员进行为期 1 天的计划培训、演练和总结。鉴于“嘉庚网”尚处于完善阶段，因此本计划仅考虑了一个Ⅰ级事件演练和一个Ⅲ级事件演练，详情参见附件 E。

7．附件

附件A　南海大学信息安全应急响应工作机构

南海大学信息安全应急响应工作机构如下所示。

一、应急响应领导小组

组长：　　副组长：

成员：

二、应急响应实施小组

组长：　　副组长：

成员：

三、应急响应日常运行小组

组长：　　副组长：

成员：

四、应急响应专家小组

组长：　　副组长：

成员：

附件B　联系人清单表

“南洋烽火”计划联系人清单表如表 11.7 所示。

表 11.7　“南洋烽火”计划联系人清单表

小组名称	姓　名	在小组中的职位	联络信息				
			工作电话	家庭电话	手　机	电子邮件	家庭地址

附件C　重大信息安全事件报告表

南海大学重大信息安全事件报告表如表 11.8 所示。

表 11.8　南海大学重大信息安全事件报告表

重大信息安全事件报告表	
报告时间：　年　月　日　时　分	
单位名称：	报告人：
联系电话：	通信地址：
传真：	电子邮件：
发生重大信息安全事件的信息系统名称及用途：	
负责部门：	负责人：
重大信息安全事件的简要描述（如以前出现过类似情况也应加以说明）：	
初步判定的事故原因：	
当前采取的措施：	
本次重大信息安全事件的初步影响状况：	
事件后果：	
影响范围：	严重程度：
值班电话：	传真：

附件D　重大信息安全事件应急响应结果报告表

南海大学重大信息安全事件应急响应结果报告表如表 11.9 所示。

表 11.9　南海大学重大信息安全事件应急响应结果报告表

信息安全事件应急响应结果报告表	
原事件报告时间：　年　月　日　时　分	
备案编号：　年　月　日　第　号　总第　号	
单位名称：	联系人：
联系电话：	通信地址：
信息系统名称及用途：	
已采用的安全措施：	
信息安全事件的补充描述及最后判定的事故原因：	
本次信息安全事件的初步影响状况：	
事件结果：	影响范围：
严重程度：	
本次信息安全事件的主要处理过程及结果：	
针对此类信息安全事件应采取的保障信息系统安全的措施和建议：	
报告人签名：	

附件E　重大信息安全事件应急响应演练方案——病毒事件应急演练

1）应急事件列表

演练场景设置：病毒造成服务器、网络设备死机；影响南海大学教职工登录“嘉庚网”或互联网。

病毒应急事件列表包括如表 11.10 所示的两个方面。

表 11.10　病毒应急事件表

事 件 分 类	事 件 描 述	应 急 分 级
“嘉庚网”管理系统事件	1．病毒造成服务器、网络设备死机	Ⅰ级
	2．影响学校教职工登录互联网	Ⅲ级

2）发现应急事件

病毒事件的发现途径主要有以下 3 种方式：

（1）“嘉庚网”用户使用终端发现异常；

（2）网络信息中心运行维护人员对“嘉庚网”进行巡检的过程中，发现异常情况；

（3）“嘉庚网”主机房自动检测系统发现异常情况。

应急演练指挥部可选择其中一种或多种事件进行演练。

3）启动应急响应

应急响应领导小组在接到紧急事件通知后，由应急响应领导小组依据病毒应急响应事件列表初步判断应急事件等级，根据应急事件的不同等级分别启动相应的应急响应方案，参考不同等级应急事件的处理方式。

4）应急事件处置

依据病毒应急事件列表，应急事件处置流程如下。

（1）病毒造成“嘉庚网”主服务器群和核心网络设备死机。

应急分级：Ⅰ级

响应时间要求：Ⅰ级应急事件需要立即响应，应急响应处理部门应立即组织技术人员在 1h 内到现场。该事件如果在 4h 之内仍未处理，将作为重大信息安全责任事故上报上级主管部门。

参与人员：Ⅰ级应急事件响应，立即组织故障所涉及各个层面所有相关单位人员参与，共同组建事件处理小组，该小组成员可包括应急响应实施小组、应急响应日常运行小组、应急响应专家小组及来自于厂商的人员。

汇报层次：Ⅰ级应急事件应逐级汇报给应急响应领导小组组长，所有事件处理过程和事件处理状态都需要在第一时间通知事件处理小组成员，整个事件响应由应急领导小组组长统一协调。事件处理告一段落之后，授权“嘉庚网”新闻栏目对校内、外发布新闻。其他人员一律不得擅自对外发表个人意见。

调用资源：Ⅰ级应急事件响应需要在南海大学相关部门及故障系统所属单位内调动资源。以首先解决故障问题为原则，保障事件得到快速解决。严重应急事件响应需要及时调用备份设备资源时，领取临时设备，保证系统尽快恢复运转。

事件处理：

① 立即停止服务器所运行的所有程序和相关服务，防止病毒进一步扩散，通过控制防火墙的策略，不要向外部发送任何数据；通过 SNMP 协议进行联动，可以切断感染主机同内网的其他主机的通信，防止感染主机在内网的大肆传播，以防止病毒的传播，并通知系统维护人员和应急响应专家小组（由南海信息安全技术中心和“巨浪”数据恢复技术中心专家组成）。

② 在感染病毒的计算机上运行杀毒软件，全面检查计算机系统，将病毒彻底清除；在感染的网络设备上，立即检查感染的端口和服务是否有异常出现，并将其关掉。

③ 在服务器查杀病毒的同时，所有服务器管理的计算机都要进行病毒查杀。

④ 如需要，启动备份服务器，同时将原有服务器与网络彻底断绝物理联系。

⑤ 如果病毒将系统破坏，导致系统无法恢复，应将感染病毒的计算机上的重要数据备份到其他存储介质，确保计算机内重要的数据不会丢失。

⑥ 对备份的数据也要进行病毒检测，防止病毒再次感染其他计算机。

⑦ 如有重要数据无法恢复，经主管领导同意后，可与“巨浪”数据恢复技术中心联系，由他们来协助恢复，需要保证数据信息不泄露，并在安全员处做记录；如为高度涉密数据，不允许由其他单位来恢复数据。

⑧ 整个事件处理完成后填写《南海大学重大信息安全事件报告表》（见表 11.8）和《南海大学重大信息安全事件应急响应结果报告表》（见表 11.9）。

（2）影响学校教职工登录互联网。

应急分级：Ⅲ级

响应时间要求：Ⅲ级事件由网络信息中心（即应急响应日常运行小组）负责处理，若 8h 之内仍未解决，上升为Ⅱ级事件并自动激活Ⅱ级事件响应流程。

参与人员：Ⅲ级事件响应由网络信息中心组织检查“嘉庚网”外联 Internet 端口及日志记录，通知中国电信南海分公司网管中心使用 SmartBit 分析仪协助分析。

汇报层次：由于Ⅲ级事件不属于重大信息安全事件，因此事件处理完成之后，由网络信息中心有关人员在当天的工作日志中进行描述即可。

调用资源：Ⅲ级事件响应需要网络信息中心下属部门及故障系统提供商 IBM 大中华区南海分公司、中国电信南海分公司网管中心提供技术支持。

事件处理流程：

① 使用主机杀毒软件或网络版杀毒软件（及时更新到最新的病毒库）对重点防范的服务器和计算机进行杀毒扫描，并将病毒彻底清除；

② 及时通知所有可能受影响的校内单位和人员，并将详细杀毒根除病毒的方法公布在“嘉庚网”网站校园新闻栏；

③ 通过控制防火墙的策略，对感染主机的对外访问数据进行控制，防止病毒对外网的主机进行感染；

④ 通知网络管理员，对病毒进行分析后，通过配置 X-Scan 来对网络进行漏洞扫描，通知存在漏洞的主机下载补丁程序进行漏洞修复；

⑤ 整个事件处理完成后填写《安全员处理记录》。

11.4　本章小结

- 应急响应的概念
- 应急响应与应急响应计划的关系
- 应急响应计划的 3 个环节
- RTO/RPO 的概念

- 确定 RTO/RPO 的难点
- 应急响应计划的准备工作
- 风险评估与业务影响分析
- 应急响应计划工作中要处理好的 3 个关系
- 应急计划得以执行的保障条件
- 呼叫树
- 安全事件的分级
- 安全事件的通告
- 应急计划的启动与分级响应
- 应急计划的培训、演练、总结和更新

尾声：如何变“惊慌失措”为“从容不迫”

如何变“惊慌失措”为“从容不迫”的答案其实只有 4 个字。哪 4 个字？

这是一个剧变的时代。

这是一个剧变的国度。

整天急促变化的是飞快旋转和移动的一切——快速涌现的汽车、风驰电掣的城际高速列车、横空越过的新一代喷气式大型客机……生龙活虎的建筑工地，也许还有人们从早到晚行进的脚步。

我们的工作节奏是高速的，我们的生活步调是快速的，我们缺乏静下心来沉思默想的时光，以至于没想到我们什么时候会渴，所以就临渴掘井；没有想到什么时候会突然响起惊雷，下起暴雨，所以不能未雨绸缪。

是的，那 4 个字的答案，就是未雨绸缪，或者事预则立。这就是做到“从容不迫”的关键，这就是“应急响应”的关键。

观感

（1）风险分析与业务影响分析是什么关系？

（2）请登录中国 CNCERT/CC 网站，查看其主要业务范围。

（3）登录其他国家 CERT 网站，查看其在世界各国的分布情况和主要业务范围。

（4）试比较分析中国 CNCERT/CC 与世界其他国家 CERT 组织的异同，如漏洞库发布信息和威胁发布信息等。

（5）地震发生后供参考的自救/互救经验是：“先轻后重、先近后远、先青年后老少”。从这些原则中您可以获得什么启迪？

（6）请在网上查阅《国家突发公共事件总体应急预案》和《国家通信保障应急预案》等权威文档，并根据您所在单位实际情况（如学校校园网）制定相应的信息安全应急计划。

（7）假设国家电网信息系统遭受Ⅰ级事件的破坏，您认为应急响应计划的重点是什么？灾难恢复计划的重点是什么？如果是华东电网信息系统呢？如果是您所在城市的电网信息系统呢？

第 12 章

法律和法规





汉谟拉比法典

入境而问禁，入国而问俗，入门而问讳。

——《礼记·曲礼上》

序幕：神话世界中需要秩序吗

依靠自觉来维护秩序是道德，依靠惩戒来维护秩序是法律。

公元前 1 700 年左右，古巴比伦王国。世界上第一部完整的成文法典《汉谟拉比法典》（The Code of Hammurabi）正式颁布实施，那时候全球人口约为 2000 万。

公元前 400 年左右，春秋战国。中国第一部完整的成文法典《法经》颁布实施，那时候中原大地的人口也约为 2000 万。

是那块诞生了“空中花园”和《一千零一夜》的土地上的人们更守规矩？还是这方孕育了“山海经”和《西游记》的国度上的人们更有道德？仁者见仁，智者见智。喜欢创造神话是人类的天性。然而到了 20 世纪末，人类第一次发现在我们自己创造的“人月神话”世界里，却需要真实的法律去维护秩序。但这又应该是些什么样的法律呢？

要点：本章结束之后，读者应当了解和掌握

- 什么是计算机犯罪？
- 计算机犯罪包括哪些内容？
- 美国近年来在信息安全立法方面有哪些特点？
- 中国信息安全立法的历史和现状是什么？

12.1 计算机犯罪概述

谈到计算机犯罪，人们自然会联想到“黑客”。然而，国外有的研究者认为近代黑客产生的历史可以追溯到 19 世纪北美长途电话公司接线生的一些恶意行为。尽管这些以侵犯长途电话公司商业利益的行为被后来的黑客们所继承，但今天人们所描述的计算机犯罪通常是指依托现代计算机网络等从事的犯罪活动。

计算机犯罪。计算机（网络）是犯罪活动所利用的资源、工具、目的或者干脆就是犯罪活动的场所（Cybercrime），其本质是指计算机（网络）是犯罪活动必要的组成部分。

计算机犯罪的方式可谓五花八门，包括（但远远不限于）以下 8 个方面。

（1）恶意代码传播（Malware/Malicious Code）。尽管在 Robert T. Morris 之前还有其他人以身试法，但 Robert T. Morris 的“知名度”似乎更高，他也是美国《计算机欺诈与滥用法案》（Computer Fraud and Abuse Act）1986 年颁布实施以来被判刑的第一人。虽然古人云“不知者不为罪”，但 Morris 却为了他的好奇心付出了 3 年牢狱、400 个小时社区义工服务外加 10050 美元的罚款。Morris 刑满释放后，又发奋攻读耶鲁大学的博士，毕业后继续从事 IT 行业工作。目前，Robert T. Morris 在 MIT 计算机系任教，但研究方向却和他“无意中”开创的网络安全领域没有直接关系了。



自从现代系统论创始人维纳（Norbert Wiener）和他的同事从古希腊文化中获取灵感，“杜撰”出 Cybernetics（系统论）这个英文单词以来，人们也往往将 Cyber 这个前置词与其他单词组合起来，形成系列的 Cyber 用语，如 Cyberspace（虚拟空间）、Cyberwar（虚拟战争）、Cybertrust（虚拟可信）等。因此在许多文献中，计算机犯罪也与 Cybercrime 同义。

（2）恶意网络堵塞攻击（Denial of Service Attack）。虽然 Morris 是该类攻击的始作俑者，但给现代社会带来引人注目的影响还是发生在 2000 年针对 Yahoo、Amazon、CNN 等商业和传播媒体网络的攻击，导致这些商业或媒体网站长时间无法提供正常服务。美国联邦调查局（FBI）和加拿大皇家骑警（RCMP）最后锁定加拿大一个网名叫“黑帮小子”（MafiaBoy）的少年，他与 CNN 网站被攻击有关。2002 年，该少年被加拿大蒙特利尔青少年法庭（the Montreal Youth Court）判处入狱 1 年，外加 8 个月的管教和禁止使用 Internet。

（3）信息战（Information Warfare）。严格地讲，由于信息领域与国家利益密切相关，所以现在还没有一位黑客由于信息战而被任何国家自己的法庭提出诉讼。然而与此相关的案例包括 1996 年一名以色列少年黑客攻击美国五角大楼网络的事件，FBI 向以色列政府提出引渡这位少年的要求，但以色列政府予以断然拒绝，后来该少年加入了以军特种部队，并被授予团级军官的军衔（引自科教片“信息战”）。

（4）网络恐怖主义犯罪（Cyber Terrorism）。这是利用网络进行传统恐怖主义犯罪活动的领域，犯罪分子往往带有明显的政治目的。例如，“基地”组织通过网络发布的各种信息和血腥视频。

（5）网络钓鱼（Phishing）。网络钓鱼技术最早出现在 Felix 等人提交给 HP 公司主办的一次国际会议的论文集中。该技术现在已经成为最猖獗的计算机犯罪形式之一，案例也很多，近年来世界各国立法机关均加大了对此技术的打击力度。

（6）欺诈与盗窃（Fraud and Identity Theft）。这种犯罪分子的动机是传统的，即为了经济利益，但犯罪手段是新型的，即利用计算机网络的脆弱性。例如，1989 年 Franklin Darden 等侵入美国南方贝尔电话公司（Bell South's Telephone）信息系统，包括北美地区的应急电话 911 系统，意图窃取该公司的长途电话卡资料。

（7）虚拟犯罪（Virtual Crime）。虚拟犯罪的作案对象是虚拟空间，作案现场也是虚拟空间。对于“大名鼎鼎”的 Kevin Mitnick 而言，20 世纪 80 年代初和 90 年代初曾因计算机犯罪先后两次被 FBI 送进了监狱，“两进两出”的他又瞄准了 Motorola、Nokia、Novell、Fujitsu 等 IT 公司的核心软件，1999 年“三进宫”。现在 Mitnick 终于洗心革面，开办了一家安全咨询公司，然而开张不久，公司的网页又被黑客篡改了……

（8）炫耀犯罪（Showoff Crime）。一般而言，炫耀是人类的一种心理活动，与犯罪扯不上关系。对于那些初次进入虚拟空间而又被迷惑得眼花缭乱的人而言，显示自己的存在价值更是一种自然的心理表现。然而却有不少人为此付出了沉痛而又真实的代价。“5 • 12”汶川大地震发生后，正当情况不明、信息不通的民众人心惶惶之时，西安亚欧学院大学生贾某侵入陕西省地震局网站，并冒充地震局发言人在其上发布了虚假的强地震预报消息，引起社会恐慌。2008 年 8 月 29 日，西安雁塔区法院以“编造、故意传播虚假信息罪”，一审判处贾某有期徒刑一年零六个月。

还有其他形形色色的新的计算机犯罪方式，如利用网络进行洗钱和“网络黑恶势力”等。如果要用一句话来形容关于计算机犯罪的态势，那就是计算机犯罪是人类真实社会中各种犯罪方式在虚拟社会中的体现。随着网络的进一步发展，完全可以预计各种新型的犯罪方式还将不断涌现。因此，世界各国法律界均对预防和惩治这些犯罪方式、规避信息安全风险、整顿（虚拟）社会秩序做了大量的工作。然而，有关信息安全的法律和法规多得浩如烟海，已经形成了一个专门的学科体系，本书不可能对其进行详细、系统的介绍。所以我们不得不结合本书的主要内容，如信息安全测评和风险评估等，对其中有代表性的法律和法规进行一个简介，请读者谅解。

12.2　信息安全法律和法规简介

由于篇幅所限，本节将简要介绍一下国内外有关计算机/信息安全及与信息化社会有关的几个法律和法规，其目的并非是对这些法律和法规的条款进行详细解释（这也是本书力所不能及的），而是希望读者从中领略到我们在进行相关法律和法规建设的时候需要借鉴的经验，正所谓“他山之石，可以攻玉”。

12.2.1　美国有关法律

1．美国联邦政府信息安全管理法案（The Federal Information Security Management Act FISMA）

“9 • 11”事件之后，美国联邦政府更加“未雨绸缪”，加强了对国家基础设施的安

全保护，其中对国家基础设施信息系统的安全保护是重中之重。2002 年，美国国会通过了《联邦信息安全管理法案》（FISMA）。FISMA 是美国《2002 年电子政务法案》的第三部分。FISMA 要求美国联邦政府所属机构每年必须对其信息安全工作进行独立的评估，以确认其有效性。评价的次数根据该部门信息系统面临的风险而定，但不能少于每年一次。这种评估包括对各政府部门在信息安全管理、运行和技术 3 个方面的控制措施。在独立评估的基础上，美国联邦政府管理与预算局应向美国国会汇报总体评估结果，美国联邦审计署则负责向美国国会汇报联邦政府各部门信息安全策略和实践的有效性及相关要求的执行情况。FISMA 的目的是为了以一种低成本并且及时、有效的方式来把信息安全风险控制在可接受的范围之内。美国国家标准和技术研究所（NIST）则出台了相关的配套评估标准，供独立评估机构遵照执行。评估过程大致分为 9 个步骤。

（1）对需要保护的信息进行分类；

（2）选择最小的控制基线（baseline）；

（3）使用风险评估过程来重新修改原有的安全控制；

（4）在系统安全计划中用文档形式把控制措施描述出来；

（5）在合适的信息系统实施安全控制；

（6）一旦安全控制付诸于实施，评估安全控制的有效性；

（7）决定部门业务战略的风险等级；

（8）赋予信息系统管理部门处理的权力；

（9）在一个可持续的基础上监督安全控制措施。

截至 2008 年，FISMA 法案已经实施了 6 年，各部门的评估结果经过“脱密”处理之后，也向全世界公布。这里需要向读者指出的是，尽管 FISMA 法案是世界范围内首部与信息安全风险评估密切相关的法律，但在实施过程中也需要不断完善。Paul Kurts 曾是美国白宫国家安全智囊团和国土安全部智囊团成员。2008 年，他在美国国会举行的 FISMA 法案执行情况听证会上做了一个发言，对 FIMSA 实施几年来的情况进行了一个总体评价，具有一定的代表性。他认为 FISMA 法案在美国联邦政府机构信息安全保障工作方面发挥了开创性作用［类似于中国中共中央办公厅、国务院办公厅联合下达的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27）号文所发挥的作用］。在 2000 年的时候，美国联邦政府对其信息系统的整体安全也是“心中无数”：没有相应的标准，缺乏全局数据，各部门对自己投入了多少人力、物力和财力来应对安全问题也知之甚少。而这一切均因 FISMA 的出现而改变。

在肯定了 FISMA 的作用之后，Paul Kurts 着重谈了关于 FISMA 存在的 4 个不足之处。这些观点对目前中国信息安全保障工作也有一定参考价值。

（1）**误导评分**：FISMA 的实施，并没有描述美国联邦机构信息安全现状是否获得了改善。该法案的实施仅仅衡量了各政府部门是否**参与了**安全评估、测试和管理的过程。例如，各部门仅仅是形成了若干份能使他们获得高分的评估报告（即使他们的信息

系统并没有通过相应的测试）。与此同时，对这些系统的评估标准和技术也是千差万别的（特别是外包给各个服务商的时候）。

（2）**狭隘评价**：FISMA 并未准确地记录和衡量一个尽责的政府部门如何在保障他们的信息系统安全方面所做的努力。例如，美国内政部的 CIO 就抱怨说，他们在 2005 年成功抵御了 40 亿次的嗅探、扫描和攻击，但这些均未体现在 FISMA 对该部门的报告中。因此，许多人质疑 FISMA“以点带面/千篇一律”（one size fits all）应对安全的模式并不适用于不同的政府部门和不同的业务战略。

（3）**整改乏力**：在过去的 5 年中，美国国会根据 FISMA 报告对美国联邦政府中最庞大的 3 个部门——国务院、国防部和国土安全部的信息安全状况打了低分，但却没有发现这些部门在信息安全方面有改进的现象。美国联邦审计总署的评价是：“许多政府部门没有足够的意愿和有效的措施来对其信息系统进行例行的安全评估”。由于联邦预算管理办公室（OMB）的职能有限，从而使得没有强制性的措施来让那些未能“达标”的部门进行整改。

（4）**嗅觉迟钝**：FISMA 实施过程中经常出现对新技术趋势的漠视。尽管“软件是一种服务”（software as a service）这一理念在 IT 界获得了越来越多的认可，但 FISMA 和 NIST 均未对此进行相应的调整。由于联邦政府的安全管控措施对那些可以联网的软件并不认可，所以很多政府机构很轻率地就回绝了许多安全解决方案，即使这些方案事实上对政府部门的信息安全大有裨益。这就造成了“第 22 条军规”的尴尬场景：由于 FISMA 和 NIST 均未将新的技术纳入考量范围，政府部门对它们的采用也就兴趣索然，从而也就导致政府信息系统办事效率低下和安全防护水平薄弱，如此恶性循环下去……

Paul Kurts 在听证会上向国会议员们提出的一个最主要的建议是：在联邦政府机构实施 FISMA 的时候，应该纳入 ISO 27001 标准（将在本书第 13 章对此进行介绍），运用 ISO 27001 标准“可定制化”的特点来解决 FISMA“以点带面/千篇一律”的缺陷。他甚至建议应该将 ISO 27001 标准和 FISMA 等同对待，提倡在联邦政府各部门中推广 ISO 27001 标准的认证工作。

2．美国《Sarbanes-Oxley法案》

“9・11”事件的发生撞毁了纽约世贸大厦，纽约证交所也感受到了“余震”。2002 年，美国著名的 Enron 公司和 WorldCom 公司又因金融丑闻和违反美国联邦政府安全法律的犯罪行为，给美国国内金融市场带来更大的动荡。为此，美国国会颁布了一项称为“Sarbanes-Oxley Act”的法律以加强公共贸易公司财政记录保留和报告的责任。尽管该法案表面上似乎与 IT、甚至信息安全毫无关系，但事实上其潜在影响正在许多企业，特别是上市企业身上显现出来。

该法案要求企业必须依靠 IT 基础设施预防相应的信息泄露情况，最大限度地确保企业的运营安全与合法经营。

该法案要求企业的 CEO 和首席财政官（CFO）承担公司的财政报告和记录系统完

整性和精确性的直接和个人的责任。

根据这一法案，在美国上市的海外公司及美国本土的中小型公司，其向美国证监会提交的财务报告必须真实可靠，必须保证与财务相关的内控有效，否则有可能被处以 100 万～500 万美元的罚款，甚至面临 10 年或 20 年监禁的重刑（相当于美国持枪抢劫的最高刑罚）。

3．美国《爱国者法案》（USA Patriot Act of 2001）

由于受“9.11”事件的强烈刺激，美国联邦政府在应急响应方面迅速启动了一系列相关法律制定的程序。《爱国者法案》就是其中影响最大的法案之一，仅仅经过 45 天，就完成了所有立法程序并于 2001 年 10 月 26 日由美国总统布什签署。

《爱国者法案》从法律上给予美国执法机构（如 FBI、CIA、NSA 等）广泛的权力和相应的设施以防止、侦破和打击恐怖主义活动。美国等西方国家历来重视对个人信息隐私的保护，在以前的法律中，政府部门调查人员即使有明确的怀疑对象，但仍然无权搭线窃听嫌疑人的有线通信系统（在北美地区，由于历史的原因，有线电话普及率远远高于手机）以确定是否有违反《计算机诈骗和滥用条例法案》（Computer Fraud And Abuse Act of 1986）的行为。但爱国者法案规定了几项具体的犯罪行为，在严重违反计算机诈骗和滥用条例的行为中，调查人员即使没有嫌疑对象，仍有权窃听有线通信系统。以往在《电子通信隐私权法案》（ECPA，Electronic Communications Privacy Act）中，规定了执法人员可以访问存储电子通信信息，如 E-mail，但不可以访问存储有线语音通信信息，如语音邮件。但现在，窃听法令首先规定了允许这些行为，其“有线通信”的定义包括了存储语音通信。因此，调查人员可从法官那里获得搭线窃听的授权，以审查语音邮件或电话应答信息（answer machine）。最初制定 ECPA 法案时，没有预见到的会产生存储语音通信这种混合数字消息系统（如数字语音邮件）。《爱国者法案》改变了窃听法令和 ECPA 法案对存储语音通信的监听方式。它从“有线通信”的定义中删除了“电子存储”而加入了相关条文，以确保存储有线通信作为存储电子通信适用于同一法规，从而允许调查人员使用通常意义的授权搜查而不是通过窃听命令来搜寻上述信息。因此，该项条款的争议性很大。

《爱国者法案》中另一项引发强烈质疑的是搜查记录条款。根据这项条款，联邦调查局人员具有获取各种商业活动记录的权力，前提是只要提出这些记录与调查外国情报或恐怖分子有关（这是再容易不过的一个理由了），因此这项取证工作的范围就拓展到包括图书馆、大学、书店和音像店的各种商业活动记录。

《爱国者法案》特别重视对网络恐怖活动的制止和预防。法案对《计算机诈骗和滥用法案》做了大量的更改，增加了对黑客的惩罚（从 10～20 年），对黑客只是意图造成伤害的行为给出了明确的定义。它针对几项特别的计算机犯罪制定了新的条例，如以国家安全或犯罪司法系统为目标的犯罪行为。为了威慑计算机犯罪分子，它也允许对计算机犯罪采取数罪并罚的形式。

《爱国者法案》2005 年年底到期，但美国国会随后通过了一个特别法案，将《爱国者法案》中的 14 项条款永久化，另两项条款的有效期将延长 4 年。法案还增加了一些保护公民自由权利的条款。并由布什总统签署后正式生效。

由于《爱国者法案》对公民的自由造成侵害，因而引起了上至共和、民主两党，下至普通民众的不满和忧虑。人们尤其对延期条款中争议最大的上述两项极为不满，认为这两项条款对美国传统中强调的个人自由构成了严重威胁。目前，美国各地已经有上百个司法管辖区颁布决议和法令，谴责《爱国者法案》对民权构成侵犯。

尽管《爱国者法案》存在一些弊端，但它也反映了美国法律界、IT 界应对新型安全威胁（非传统安全威胁）的一些前瞻性的法律思考，值得中国有关方面仔细研究，而不能“因噎废食”、一概而论。

4．美国《计算机安全法案》（The computer Security Act of 1987）

美国《计算机安全法案》的新颖之处在于试图通过确立基线（baseline）的安全实施方案来保护联邦计算机系统的法律。所谓“基线”是指至少要满足的条件，但允许根据实际情况增加安全措施。《计算机安全法案》由美国国家标准局（NIST）与美国国防部国家安全局（DOD/NSA）合作承担，目的是：

（1）为计算机系统制定标准、指南和相关的方法与技术；

（2）为大多数的联邦计算机系统制定统一的标准和指南；

（3）从成本效益的角度，为联邦计算机系统内敏感信息的安全性和保密性制定技术、管理、物理和行政标准与指南；

（4）对于装有敏感信息的联邦计算机系统，制定员工培训指南，以供系统操作员在安全培训中使用；

（5）通过调查研究并与其他国家的政府和私人/机构进行合作，制定标准和指南的确认程序，并评估它们的有效性。

除了 NIST 和 NSA 之外，美国商务部（Department of Commerce）也成立了一个计算机系统安全与保密顾问委员会，为《计算机安全法案》的实施提供咨询。这个委员会主要负责确定新出现的有关计算机系统安全和保密的各种管理、技术、行政和物理安全问题，并就这些问题向标准局（Bureau of Standards）和商务部秘书提出建议。该委员会负责向商务部秘书、联邦政府管理和预算办公室（Office of Management and Budget）负责人、国家安全局负责人和国会的相关委员会报告。

《计算机安全法案》也对 1949 年《联邦财产和管理服务法案》（Federal Property and Administrative Services Act of 1949）做了修正。该修正案要求国家标准局发布联邦计算机系统的相关标准和指南，并让这些标准在重要部门得到强制性实施。

《计算机安全法案》的另一条款要求是必须对员工进行计算机安全的定期培训，培训内容包括计算机安全意识、计算机安全实施方案的适合性等；培训对象是那些所有涉及联邦政府计算机系统管理、使用或运行维护的雇员。对联邦政府雇员的培训旨在提高

他们对计算机系统所面临的威胁和脆弱性的意识，并鼓励他们使用改进的计算机安全实施方案。该项条款针对“谁负责计算机系统安全和保密性”、“敏感信息系统的识别”和“提出正式的安全计划需求”等问题，为美国联邦政府机构提供法律指南。

5．美国《计算机诈骗和滥用法案》（Computer Fraud And Abuse Act of 1986）

20 世纪 80 年代中期，正是计算机从大型机（main frame）向个人用户终端这块处女地大力开疆拓土的时候。计算机开始快步走出国防军事、前沿科研等“象牙塔”，变成了“下里巴人”也能接触和使用的普通电器，从而也出现了人类历史上各种犯罪行为向虚拟空间延伸的趋势。为此，美国制定了《计算机诈骗和滥用法案》。该法案涉及与计算机有关的诈骗和相关活动，重点界定了以下犯罪行为。

（1）任何人未经授权访问计算机或超出了访问权限，并通过该行为获取由美国政府根据总统法令限制的信息。

（2）上述信息出于保护国家安全、维持外交关系或者为了保护保密数据资料的目的，已经被要求限制而未经授权向外披露。

（3）如果有理由认为这些信息可能被用于损害美国政府或其他外国政府的利益，被蓄意地扩散、传递、传播或导致保密信息被扩散、传递、传播的行为。

（4）那些试图扩散、传递、传播或导致这些信息被扩散、传递、传播给无权访问的人员，或是蓄意地持有这些保密信息而没有把它交给有权访问该信息的美国政府官员的人员。

（5）任何人未被授权访问计算机或超出访问权限，从而获取金融机构和信用卡发行商的财政记录信息，或者一些美国政府机构的信息，或者其他一些受保护计算机内的信息。

（6）任何人未经授权地访问美国政府机构的非公开计算机，或者访问由美国政府机构专门使用的计算机，或者即使并不是美国政府的专有资产，但由美国政府使用的计算机，而这种行为会影响政府使用这些计算机。

（7）任何人故意地试图欺骗、访问未向其授权的计算机，或超出访问权限，并通过这种行为试图进一步地诈骗以获取有价值的信息。

（8）任何人有意地传播恶意的程序、消息、代码或命令，而且由于这些故意的擅自行为对受保护计算机造成损害。

（9）任何人故意地擅自访问受保护计算机系统，其行为造成损失。

（10）任何人故意地使用某种密码或类似信息以进行欺骗交易的行为而影响了贸易活动，并使用该方法擅自访问美国政府使用的计算机。

（11）任何人故意地向任何个人、公司、协会、教育机构、金融机构、政府实体或其他合法实体敲诈财物，故意在贸易活动中传播带有威胁的信息并损害了受保护的计算机系统等。

2001 年，美国国会通过的《爱国者法案》对《计算机诈骗和滥用法案》进行了大量

的修改。

6．美国《通信规范法案》（Communications Decency Act）

在捍卫传统社会价值观、遏制各种利用现代通信工具进行色情淫秽信息传播、干扰他人正常生活、保护未成年人健康成长等方面，美国出台了《通信规范法案》，要点是如下所述。

（1）在国内各州和国外通信中，任何人采用电子通信设备故意制造、煽动和传播淫秽、色情和下流的评论、邀请、提议、建议、图像和其他信息，故意骚扰、辱骂、威胁或烦恼他人，应当受到罚款或监禁两年或两年以下（或两者并罚）。

（2）任何人采用电子通信设备故意制造、煽动和传播淫秽、色情、下流的评论、邀请、提议、建议、图像和其他信息，并且知道信息的接收者未满 18 岁，不管信息的制造者是打电话或是发起这些信息与否，应当受到罚款或监禁两年或两年以下（或两者并罚）。

（3）任何人通过电话或利用电子通信设备，不透露自己身份故意骚扰、辱骂、威胁或烦恼受话者或信息接收者，不管会话或通信继续与否，应当受到罚款或监禁两年或两年以下（或两者并罚）。

（4）任何人让他人电话重复不断地响铃，故意让对方烦恼；或者通过重复地打电话给他人或通过电子设备发起通信去骚扰对方，期间发生了会话或通信行为者，应当受到罚款或监禁两年或两年以下（或两者并罚）。

（5）任何人有意地允许其通信设备在他控制范围内用于任何非法活动，或者意图用于这些非法活动，应当受到罚款或监禁两年或两年以下（或两者并罚）。

（6）任何人在美国采用电话方式，直接或通过录制设备以商业为目的有意制造淫秽信息，不管制造者打了这种电话与否；或者允许其电话在他控制范围内用于非法活动；都应当受到罚款或监禁两年或两年以下（或两者并罚）。

（7）任何人在美国采用电话方式，直接或通过录制设备以商业为目的有意制造猥亵信息给未满 18 岁者，或者未经他人同意擅自传给他人，不管制造者打了电话与否；或者允许其电话在他控制范围内用于非法活动。都应当受到罚款至多 50000 美元或监禁至多六个月（或两者并罚）。

（8）在国内或国外通信中，任何人故意使用计算机交互服务，向特定的人或未满 18 岁者发送任何淫秽、色情、下流的评论、邀请、提议、建议、图像和其他的信息，依据当代社会评判标准，在以上的传播信息中公然地描述色情的性行为或性器官，不管这些服务的用户打了电话或进行了通信与否，应当受到罚款或监禁两年或两年以下（或两者并罚）。

（9）任何人有意地允许其通信设备在他控制范围内用于任何非法活动，或者意图用于这些非法活动，应当受到罚款或监禁两年或两年以下（或两者并罚）。

7．美国《隐私权法》（The Privacy Act）

1974 年 12 月 31 日，美国参众两院通过了《隐私权法》，1979 年，美国国会在修订《联邦行政程序法》时将其编入《美国法典》第五编“政府组织与雇员”。该法是美国行政法中保护公民隐私权和了解权的一项重要法律。《隐私权法》就联邦政府机构对个人信息的采集、使用、公开和保密问题做出了详细规定，以此规范联邦政府处理个人信息的行为，平衡公共利益与个人隐私权之间的矛盾。

进入 21 世纪后，随着 Internet 的飞速发展，隐私权已成为信息安全的热点问题。在过去，采集来自不同渠道的个人信息并建立专门的数据库几乎是不可能的。但现在由于多种渠道数据的汇集，使得缺乏职业道德的机构或个人有可能建立数量惊人的个人信息数据库。许多机构把个人信息作为商品进行收集、交易和销售，普通民众开始意识到这种情况，希望政府通过立法的方式来保护他们的隐私权益。

在美国，有关保护个人隐私权的法令越来越多。然而，其中规定的公民隐私权却不是不受监视的绝对自由，而应理解为“未经法院授权，执法人员不得进行监视”。为了更好地理解这个随着技术进步而不断发展的老问题，下面将对《隐私权法》及其相关背景做一个简要介绍。

美国各种法典（当前美国法律汇编）中所陈述的一些规则已经规定了信息服务提供商保护客户信息秘密的责任。这些法规中有关客户的信息隐私权指出，任何获取到的业主信息应明确用于提供服务，而不应用于任何市场销售目的。它还规定，除非是提供服务所必需或应客户请求，电信公司不能透露个人信息。该法律允许使用由非私有（个人）信息构成的集合信息，只要这些信息是提供给所有信息服务提供商的，且它们的商业行为都采用公平竞争的方式。

因为一个机构采用把表面上无害的信息关联在一起进行分析、汇总、分类加工的方式，可以把各种来源的数据组合成更有商业价值的信息，所以使用集合信息可提高人们对隐私权的关注程度。例如，政府人口数据库与电话地址录的映射信息分布、破产法庭记录的附录参照索引等，对寻找新的商机的人来讲，这些信息将有助于他们的新颖而富有创意的商业活动。

以往美国颁布的法律、法规规定了公众服务商使用私有数据的规则，而 1974 年《隐私权法》则规定了政府使用私有信息的规则。指定该法是为了确保政府机构对个人和商业信息进行保护，如果这些信息的任何部分未经同意被对外发布，则相关机构就应对此负责。该法案声称：“任何机构都不能采用与他人或其他机构通信的方式，透露记录系统中的信息，除非是应与记录相关人员的要求或经其同意……”然而，该法案也考虑到政府部门在履行职责中对个人隐私信息的使用情况，提出下面的机构可以不受部分规定的限制，以便他们能行使他们的职责：

（1）人口普查统计局；

（2）国家档案管理局；

（3）美国国会；

（4）总审计局；

（5）某些法庭指令；

（6）征信所。

此外，该法案对个人访问其他人的信息也加以了界定，规定也可以访问被别人所控制的信息，只要他能证明这样做能保护他的健康和安全。

除了《隐私权法》之外，1986 年颁布的《电子通信隐私权法》是一个多条法令的集合，它规定了有线通信、电子和口头通信的截取侦听规则。它主要涉及以下领域：

（1）有线通信、口头或电子通信中途截取和透露；

（2）有线通信、口头或电子通信窃听设备的制造、分配、占有和广告行为；

（3）在何种情况下没收有线通信、口头或电子通信窃听设备；

（4）截取的有线或口头信息作为证据使用；

（5）对有线通信、口头或电子通信截取行为的授权；

（6）对截取到的有线通信、口头或电子通信信息的透露和使用授权；

（7）有线通信、口头或电子通信中途截取侦听程序步骤；

（8）截取到的有线通信、口头或电子通信信息的报告；

（9）禁止非法截取信息的禁令。

在 2001 年通过的《爱国者法案》中对此又进行了大量的修改，从而赋予联邦政府更多的探听个人隐私的权利。

8．美国《信息自由法案》（Freedom of information Act of 1966）

美国的《信息自由法案》是在社会、政治、经济和科技事务日益复杂化，公众要求信息共享的呼声日益高涨的情况下，经过公众，特别是美国新闻界十多年的努力，于 1964 年通过的。其后，由于执行过程中发现诸多漏洞，1974 年又进行了修订。在实施过程中，又不断得到很多法庭案例的补充，现在逐渐趋向完善。《信息自由法案》的立法原则和司法实践，对西方一些国家制定和实施政务公开化的法律制度产生了较大的影响。“博采众家之长”，中国 2008 年 5 月 1 日开始实施的《中华人民共和国政府信息公开条例》也借鉴了该法案的一些成熟思想。

美国的《信息自由法案》是关于联邦政府信息公开化的行政法规。它要求联邦政府的记录和档案原则上向所有人开放，但是有 9 类政府信息可免于公开。

（1）豁免条款第一项规定：“A. 根据总统行政命令所确立的准则，为了国防或外交政策的利益特别授权予以保密的；B. 依照总统的此类行政命令事实上被恰当地归入机密类的信息，不适用本法。”

（2）豁免条款第二项规定：“仅仅与机构内部人事规则与业务常规有关的信息”不适用本法。

（3）豁免条款第三项规定：“明确地准许免予透露的信息”不适用本法（但有附加

规定）。

（4）豁免条款第四项规定：“贸易上的秘密及获得某人的特许而取得的商业上或金融上的信息”不适用本法。

（5）豁免条款第五项规定：“除了正与该机构进行诉讼的机构之外，其他当事人依法不能利用的机构之间或机构内部的备忘录或函件”不适用本法。

（6）豁免条款第六项规定：“一经透露便将构成明显地、不正当地侵犯个人隐私的人事和医疗档案材料或者类似的档案材料”不适用本法。

（7）豁免条款第七项规定：“为了执法的目的而搜集的调查记录”不适用本法（但有附加规定）。

（8）豁免条款第八项规定：“管理或监督金融机关的负责机构所准备的，或者为了此种机构供其使用而准备的检查报告书、经营报告书、情况报告书上记载的事项，或者与此种报告书有关系的事项”不适用本法。

（9）豁免条款第九项规定：“关于油井的，包括地图在内的地理学和地球物理学的情报和资料”不适用本法。

除此之外，公民可向任何一级政府机构提出查阅、索取复印件的申请。政府机构则必须公布本部门的建制和本部门各级组织受理信息咨询、查找的程序、方法和项目，并提供信息分类索引。公民在查询信息的要求被拒绝后，可以向司法部门提起诉讼，并应得到法院的优先处理。这项法律还规定了行政、司法部门处理有关申请和诉讼的时效。

《信息自由法案》只适用于美国联邦政府机构，而对于由国会、法庭或由州、地方政府机构所保留的记录却没有规定有权访问。

上面主要对美国的相关法律、法规进行了一个简介，事实上，世界各国对信息和信息安全所带来的法律问题都进行了大量有益的探索，其中有很多思想都值得中国在进行现代化、信息化建设历程中不断地研究、交流、吸收、创新和实践。

12.2.2　中国信息安全法律和法规的历史沿革

由于传统文化和历史等方面的原因，中国在进行现代“法制化国家”建设的过程中虽然面临种种阻碍，但在党和政府的高度重视下，特别是中国各级立法机构和法律界人士的不断努力下，近年来中国对信息安全有关的法律和法规的建设也逐渐加大了力度。然而，由于中国信息化建设的历史相对西方国家而言还处于初级阶段，而随着中国社会经济的飞速发展，其他事关社会民生、政治和经济建设等领域对法律的需求更为迫切，有关信息安全的法律和法规在整个法律框架中所占的比重还不高，中国在信息安全立法的研究及案例还需要进一步挖掘，信息安全法律和法规的整体框架与国家顶层法律和法规体系尚未适配，实施细节等还需不断完善。面对这一系列发展中的问题和挑战，相信本书的读者也将和我们一样以乐观、积极和前瞻性的态度面对目前中国信息安全法律和法规方面暂时存在的部分盲区，并通过各方面力量包括我们自身的努力来不断地完善这

一法律体系。下面就简要介绍中国目前几个重要的并与本书主要内容相关的法律和法规的历史演变。

从 1994 年开始到目前为止，中国信息安全法律和法规经历了 3 个阶段的建设。为了便于读者记忆，大致可以归纳为计算机系统安全阶段→互联网安全与内容安全阶段→信息安全战略阶段 3 个发展阶段。

1．计算机系统安全阶段

《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》）是中国最早颁布的专门针对信息安全领域的国家法律，1994 年 2 月 18 日，以中华人民共和国国务院令的形式颁布实施。

《中华人民共和国计算机信息系统安全保护条例》简介

《条例》共分 5 章 31 条，其主要涉及的内容包括以下 4 个方面。

（1）**管理体系**：规定了计算机信息系统安全保护的主管部门，如公安机关、国家安全机关和国家保密部门等的职责；

（2）**管理制度**：确立了中国计算机信息系统安全保护制度是等级保护制度；

（3）**管理权限**：对计算机信息系统安全监管部门的权限进行了界定；

（4）**法律责任**：对违反该条例的处罚措施进行了阐述，如对违反计算机信息系统等级保护制度、违反互联网备报制度、隐藏或延时上报信息安全事故、拒不改进计算机信息系统安全等方面，公安机关有权予以停机整顿；对故意输入计算机病毒及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款，对单位处以 15 000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1～3 倍的罚款。

由此可见，在 20 世纪 90 年代，该条例规定的中国有关执法机关对计算机病毒等方面的处罚还相对较轻，不足以威慑现在各种以经济利益、政治目标为诉求的网络犯罪活动。因此，在《中华人民共和国刑法》（简称《刑法）第 217、218、285、286、287、288 条等法律依据及最高人民法院等关于相关司法解释的基础上，一些危害信息安全的案例迅速得到裁决和审判。然而从总体上来讲，在 20 世纪 90 年代初期，中国针对计算机信息系统领域的违法犯罪活动仍然处于依托原有的《刑法》等体系进行惩处的局面，法律条款的盲区和空白之处依然较大，不适应威慑和遏制当时国际上正在涌现的各种依托 Internet 等高新技术平台进行犯罪活动的趋势。

从 1994 年之后，中国信息安全法律和法规体系开始进入了初步建设的时期。根据《条例》赋予的职责，公安部、国家保密局等信息安全主管职能部门相继制定了一大批相关法律和法规，如《计算机信息网络国际联网安全保护管理办法》（公安部，1997 年）、《计算机信息系统安全专用产品检测和销售许可证管理办法》（公安部，1997 年）、《计算机信息系统保密管理暂行规定》（国家保密局，1998 年）、《商用密码管理条例》（国务院令，1999 年）等。

与此同时，中国在这一时期对信息安全的认识正在随着各种高新技术，特别是 IT 技术的飞速发展而产生深刻的变化，从关注计算机本身的安全开始延伸到网络再到互联网的安全。

2．互联网安全与内容安全阶段

互联网安全与内容安全阶段的特点是更加重视网络及互联网的安全，也更加重视信息内容的安全。其有代表性的法律和法规包括《计算机信息系统国际联网保密管理规定》（国家保密局，1999 年）、《计算机病毒防治管理办法》（公安部，2000 年）、《互联网信息服务管理办法》（国务院令，2000 年）。全国人民代表大会在 2002 年 12 月 28 日颁布的《全国人民代表大会常务委员会关于维护互联网安全的决定》（以下简称《决定》），说明互联网信息安全已经引起了中国最高立法机关的高度重视。《决定》规定了一系列禁止利用互联网从事危害国家、单位和个人合法权益的活动。

这些法律和法规的颁布和实施，比较有效地解决了中国司法界对新型网络犯罪进行审判的法律需求，但中国信息安全法律和法规的制定之路依然任重而道远。

3．信息安全战略阶段

2003 年 7 月 22 日，国家信息化领导小组第三次会议通过了《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）（以下简称“27 号文”）。该文的颁布和实施对中国信息安全领域具有划时代的意义。在“27 号文”的影响下，中国信息安全法律体系的建设也开始进入一个更高的阶段。

“27 号文”明确了加强信息安全保障工作的总体要求和主要原则，确定了实行信息安全等级保护这一基本制度及信息安全风险评估的重要作用，强调以密码技术为基础的信息保护和网络信任体系建设，指出要建设和完善信息安全监控体系，重视信息安全应急处理工作，加强信息安全技术研究开发，推进信息安全产业发展，加强信息安全法制建设和标准化建设，加快信息安全人才培养，增强全民信息安全意识等工作重点。因此，从 2003 年开始，中国信息安全发展战略目标得以明确，各相关领域的工作任务分工更加细致。

在“27 号文”的推动下，中国在信息安全法律和法规方面也开始进入了新的起步阶段，有代表性的法律和法规包括《中华人民共和国电子签名法》（全国人大常委会，2004 年）、《电子认证服务管理办法》（信息产业部部长令，2005 年）等。我们完全可以期待，在“27 号文”的带动下，中国信息安全法律和法规建设正在进入一个崭新的阶段。

此外，中国行业主管部门和省级（直辖市）人大还根据自身实际情况，颁布实施了一系列行业或地方的法律和法规，如《重庆市计算机信息系统安全保护条例》（1998 年）、《广东省计算机信息系统安全保护管理规定》（2003 年）等。

除了上述与信息安全和本书所涉及的主要内容直接相关的部分法律和法规之外，在 2008 年新修订的《中华人民共和国刑法》修正案（七）中增加了如下的规定：“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将履行公务

或者提供服务中获得的公民个人信息出售或非法提供给他人，或以窃取、收买等方法非法获取上述信息，情节严重的，应追究刑事责任，处三年以下有期徒刑或者拘役”。在这个位于国家法律体系顶层之一的《刑法》中所体现出来的对公民隐私权的保护，是中国“以人为本”并结合新技术发展趋势的立法思想的重要体现。

最后，作为本章的结束，我们对《中华人民共和国政府公开信息条例》（简称《条例》）做一个简介，这个《条例》不仅是中国进入信息化国家的重要法律体现，同时也必将给从事信息安全工作的人员带来许多新的思考和挑战。

《中华人民共和国政府公开信息条例》简介

（1）《条例》原则：“行政机关公开政府信息，应当遵循公正、公平、便民的原则。”行政机关应当及时、准确地公开政府信息，发现影响或可能影响社会稳定、扰乱社会管理秩序的虚假或者不完整的信息，行政机关应当在其职责范围内发布准确的信息予以澄清。

目前中国各级政府纷纷建立了政府新闻发言人制度，通过政府的权威信息发布，主动向社会公众公开政府有关信息。此次突如其来的汶川大地震发生后，中国政府对毁灭性地震造成的人民生命财产的损失情况予以及时和翔实公布，就是《条例》精神的重要体现。

（2）《条例》规定：“国家行政机关不得公开涉及国家秘密、商业秘密、个人隐私的政府信息。”

《条例》要求行政机关建立健全政府信息发布保密审查机制，明确审查的程序和责任。《条例》强调，行政机关在公开政府信息前，应当依照《中华人民共和国保守国家秘密法》及其他法律、法规和国家有关规定，对拟公开的政府信息进行审查。行政机关对政府信息不能确定是否可以公开时，应当依照法律、法规和国家有关规定报有关主管部门或者同级保密工作部门确定。

世界各国立法机关都是将国家安全和国家利益置于首位的（如上面介绍的美国《信息自由法案》等），中国在制定政府公开信息的时候也体现了这一“整体利益高于个人利益”的思想。

《条例》同时规定：“经权利人同意公开或者行政机关认为不公开可能对公共利益造成重大影响的涉及商业秘密、个人隐私的政府信息，可以予以公开。”

（3）《条例》规定：“公民可主动向政府申请获取相关政府信息。”

政府部门所掌握的信息量大、面广，涉及社会生产和生活各个方面，其中有相当一部分政府信息只涉及部分人和事。基于此，《条例》规定公民、法人或者其他组织可以主动向政府申请获取所需要的政府信息。《条例》同时明确，“行政机关认为申请公开的政府信息涉及商业秘密、个人隐私，公开后可能损害第三方合法权益的，应当书面征求第三方的意见；第三方不同意公开的，不得公开。但是，行政机关认为不公开可能对公共利益造成重大影响的，应当予以公开，并将决定公开的政府信息内容和理由书

面通知第三方。”

（4）《条例》规定：“行政机关应当将主动公开的政府信息，通过政府公报、政府网站、新闻发布会及报刊、广播、电视等便于公众知晓的方式公开。”

如何在新的形势下保障电子政务公开信息的完整性、可用性等就是从事信息安全测评和风险评估的人员的使命之一。

（5）《条例》规定：“公民、法人或者其他组织认为行政机关不依法履行政府信息公开义务的，可以向上级行政机关、监察机关或者政府信息公开工作主管部举报，收到举报的机关应当予以调查处理。”

“公民、法人或者其他组织认为行政机关在政府信息公开工作中的具体行政行为侵犯其合法权益的，可以依法申请行政复议或者提起行政诉讼。”

（6）《条例》还明确了 4 类政府信息必须公开，包括涉及公民、法人或者其他组织切身利益的；需要社会公众广泛知晓或者参与的；反映本行政机关机构设置、职能、办事程序等情况的和其他依照法律、法规和国家有关规定应予以公开的信息。

可以预计，随着 4 类政府信息的分类细化和各种案例的实施，公众对其知情权的范围将更加明确，由此带来的信息安全保障服务工作也将更加细致而艰巨。

12.3　本章小结

- 计算机犯罪概述
- 美国主要信息安全立法的特点
- 中国计算机安全法律和法规建设的历史与现状

尾声：从囚徒困境说起

在博弈论中，有一个经典的“囚徒困境”。

在法律和规定下，两名囚徒（犯罪嫌疑人）有如下选择:

若一人认罪并检举对方，而对方保持沉默，此人将立即获释，沉默的对方将被判监禁 10 年;

若两人都保持沉默，则两人都被判监禁 0.5 年。

若两人都互相检举，则两人都被判监禁 2 年。

两名囚徒会如何做出选择？这并非一个简单的问题，让我们稍加分析。无论两人中的谁都会这样想:

若对方选择沉默，那么我检举对方我就会立即获释！所以，假如对方沉默我就要选择检举。

若对方选择检举我，我如果沉默就要被判 10 年监禁，太长久了，太难熬了！所以，假如对方检举我，我也要检举对方才能降低刑期（2 年刑期毕竟比 10 年好多了！）

所以这时我也得选择检举。

因此，无论什么情况，我都得选择检举。

结果呢，两人都几乎必然会这样想，于是两人互相检举，都被判监禁 2 年。

如果将上述“法律和规定”的假设稍加改动，变成“沉默者在另一人检举的情况下获刑 2.5 年（而不是 10 年）”，那么，虽然单方面选择沉默会比互相检举刑期还要长，但很可能两人都选择沉默——“犯罪（隐瞒事实）的成本很低”。

可见法律和法规的影响是多么巨大——没有严密的法律保障，“技术”可能显得那么苍白无力。在信息安全领域也是如此。

观感

（1）请查阅并统计世界各国对利用网络钓鱼（phisiong）技术进行犯罪活动的诉讼案例。

（2）请查阅近年来美国国会公布的 FISMA 评估结果。

（3）请统计、整理和分析近年来发生在中国的计算机犯罪的类型、技术特点和审批依据，给出您对未来计算机犯罪方式的预测。

（4）请在网上查阅英国、德国、日本和加拿大等国有关信息安全立法的内容并提交相关分析报告。

（5）请在网上查阅《中华人民共和国计算机信息系统保护条例》、《中华人民共和国保密法》等相关法律和法规及《中华人民共和国刑法》的相关条款，同时在网上查阅近年来中国有关计算机犯罪的案例，然后练习：①模拟法官的角色对其进行模拟审判；②模拟律师的角色，为其进行模拟辩护。

（6）您认为需要在哪些方面进一步加强中国信息安全的立法工作？您有什么建议？

第 13 章
信息安全管理体系





视觉的幻影与对称之美

Veni，vidi，vici（我来了，我看见了，我征服了）。

——凯撒大帝“小亚细亚战役”的捷报

序幕：武学的最高境界

喜爱武侠小说的读者肯定都熟悉“无招胜有招”、“臻于化境”等这样的字眼，它反映的是武学追求上的至高境界。在信息安全的“刀光剑影”之中，什么是安全学的最高境界的追求呢？

我们今天使用的防火墙、IDS、安全审计系统、门禁系统和数字证书等各种软、硬件产品，就好比冷兵器时代的“矛、锤、弓、弩、铳、鞭、铜、剑、链、挝、斧、钺、戈、戟、牌、棒、枪、扒”十八般武器，各有所长；本书前面所介绍的各种信息安全测评与风险评估技术、流程就如同各门各派的武功套路，各有所用……

当我们在信息安全的群峰之间跋山涉水，最后准备“华山论剑”的时候，哪一种武功能博采众家之长、达到“臻于化境”的境界呢？

要点：本章结束之后，读者应当了解和掌握

- 什么是信息安全管理体系（ISMS）？
- PDCA-ISMS“戴明环”有哪几个环节？
- 如何建立 ISMS 体系？
- 推行 ISMS 的工作中面临哪些挑战？

13.1 ISMS概述

信息时代的信息安全，已经从“单一的、纯技术的对抗”变成了“综合的、体系的竞争”；从“零散、无序、被动”地**应对**风险走向了“系统、连贯、主动”地**驾驭**风险。

古往今来，人类在这个星球上修筑的建筑物何止千万，它们虽然形态各异，但有一点却是亘古不变的，那就是先评估地质地理环境，然后在宁静的地层上（或下）修建起静止不动的建筑，形成一个个凝固的音符。然而有人尝试过在波涛汹涌的大海上建起随波逐流、因势而变的高楼吗？尽管这种想法在现实社会中是属于科幻小说的题材，然而在虚拟空间中我们却能够加以实现。

随着信息时代的降临，我们的日常生活和工作都越来越沉浸在信息海洋之中，因此必须寻找出一个能够在“虚拟海洋”中设计和施工大楼的方法，并能在里面（相对）安全居住。到目前为止，我们认为这种方法可能就是**信息安全管理体系**（ISMS，Information Security Management System）。

为了帮助读者理解 ISMS 的本质思想，并在今后的工作中自觉地遵循 ISMS，下面简要介绍一下 ISMS 与现代管理学的血缘关系和产生 ISMS 的历史背景。



质量体系建设的历史具有浓厚的军事色彩。第二次世界大战开始以后，由于战争的需要，美国军工生产急剧发展，尽管大量增加检验人员，但在战场上还是经常发生武器弹药的质量事故。为此，美军于 1941—1942 年间制定并公布了《质量管理指南》等系列标准，收到了显著效果。战后，前苏联也将军品生产所积累起来的质量管理经验扩展到民用部门。“老毛子的东西皮实”，中国东北的倒爷常常这样讲。进入 20 世纪 60 年代，美国和日本的许多大型企业纷纷开始系统地研究全面质量管理。1987 年，国际标准化组织 ISO 正式公布了 ISO 9000 系列质量标准。

（1）**从产品质量管理到全面质量管理。**从 20 世纪初开始，进入工业化阶段的人类社会大规模工业生产导致了对产品质量进行科学控制的迫切需求，并先后经历了以 F. W.Taylor（1911）为代表的“产品质量检验”到以 W.A.Shewhart（1924）为代表的“统计质量控制”等不同的阶段。第二次世界大战中，工业化强国如美国和苏联等对大规模军品生产过程中的质量控制提出了更加严格的要求，使得以产品质量为核心的管理进化到以费根堡姆（1961）为代表的“全面质量管理”阶段。

（2）**质量管理的国际化。**随着国际贸易的迅速扩大，产品和资本的流动日趋国际化，伴随而生的是国际产品质量保证和产品责任问题。由于许多国家和地方性组织相继发布了一系列质量管理和质量保证标准，制定质量管理国际标准已成为一项迫切的需要。为此，ISO 于 1979 年单独建立了质量管理和质量保证技术委员会（TC176），负责制定质量管理的国际标准。1987 年 3 月，正式发布了 ISO 9000-9004 质量管理和质量保证系列标准。该标准总结了各先进国家的管理经验，将之归纳和规范。发布后引起世界各国的关注，并予以贯彻，适应了国际贸易发展需要，满足了质量方面对国际标准化的需求。

（3）**信息安全管理体系。**20 世纪 90 年代中期，Internet 在全球范围内开始急剧扩张，随之而来的安全问题日趋突出，人们开始了“在信息海洋中建筑安全大厦”的探索。1995 年，英国标准协会（BSI，British Standards Institute）受英国贸工部（DTI，

The Department of Trade and Industry）委托，开始着手制定信息安全管理标准，后称为BS7799。负责标准开发和管理工作的BSI-DISC Committee BDD/2 工作组是由来自贸易和工业部门的众多代表共同组成的，其成员在各自的领域都具有较大的影响力，包括世界金融保险业的鼻祖英国保险协会（Association of British Insurers）、渣打管理会计协会（CIMA）、汇丰银行（HSBC）等，通信行业有大英电信公司，还有像壳牌（shell）、联合利华（Unilever）、毕马威（KPMG）等这样的跨国机构。该标准在短短几个月内就迅速制定完毕。同年，BS 7799-1:1995《信息安全管理实施细则》首次出版，它提供了一套综合性的、由信息安全最佳实践（best practices）构成的实施细则，目的是为确定各类信息系统通用控制提供唯一的参考基准。



1704 年，英国击败了法国，但却留下了 5 300 万英镑的巨额战争债务。随后，英国议会批准成立了股份制的“南海公司”。该公司向政府认购了 1000 万英镑的债券，解决了大英帝国的燃眉之急。政府随之投桃报李，默许该公司大量发行溢价股票。科学巨匠牛顿、英国国王乔治一世等名流纷纷加入投机行列，英伦三岛民众也趋之若鹜……最终导致伦敦金融市场崩盘。英国议会痛定思痛，为防止类似事件再次发生，通过了所谓的“泡沫法案”（Bubble Act）以规避金融风险。这就是今天“泡沫经济”一词的由来。

在随后一段时间里，由于电子商务的发展，引发了客户、供应商、贸易伙伴间对各自信息保护能力的信任问题，从而使所谓的“第三方认证”（authorized third party）应运而生。信息安全管理应遵循最佳实践，但怎样做？执行程度如何？是否完备？这就需要有一个共同的尺度来进行衡量。

1998 年，BS 7799-2:1998《信息安全管理体系规范》（Specification for Information Security Management Systems）公布，这是对 BS 7799-1:1995 的有效补充，它规定了信息安全管理体系的要求和对信息安全控制的要求，是一个组织信息安全管理体系评估的基础，可以作为认证的依据。至此，BS 7799 标准体系框架初步成型。

由于 BS 7799 日益得到国际认同，使用的国家也越来越多，2000 年 12 月，国际标准化组织 ISO/IEC JTC 1/SC27 工作组通过了对 BS 7799-1:1999 的认可审核，正式将其转化为国际标准，即所颁布的 ISO/IEC 17799:2000《信息技术　信息安全管理实施细则》，从而使其成为了国际质量标准体系的一部分。作为一个全球通用的标准，ISO/IEC 17799:2000 并不局限于 IT，也不依赖于专门的技术，它是由长期积累的一些经典的实践经验构成的，是市场驱动的结果。



PDCA 是管理学中的一个通用模型，最早是由休哈特（Walter A. Shewhart）于 1930 年构想的，后来被质量管理专家戴明（Edwards Deming）在 1950 年再度挖掘出来，并加以广泛宣传和运用于持续改善产品质量的过程当中，因此 PDCA 也被称为“戴明环”。

2002 年，BSI 对 BS 7799-2:1999 进行了重新修订，正式引入了现代管理学中一个有着 50 年历史并且久经考验的

模型——PDCA 过程模型（Plan、Do、Check 和 Act，即所谓的“戴明环”。2004 年 9 月 5 日，BS 7799-2:2002 正式发布，随即提交 ISO，并迈入 ISO 的“快速通道”（Fast Track 流程）。2005 年，BS 7799-2:2002 终于被 ISO 所采纳，并于同年 10 月推出了国际标准 ISO/IEC 27001:2005。这一个国际标准体系所对应的中国国家标准则是本章介绍的重点。图 13.1 描述了 ISO/IEC 27001:2005 的核心模型——PDCA-ISMS“戴明环”。

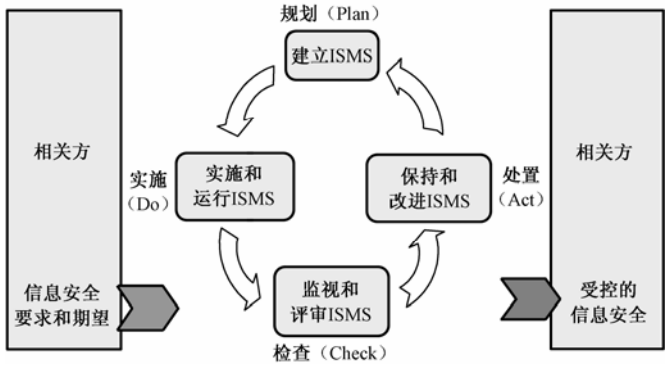


图 13.1　PDCA-ISMS“戴明环”模型

因此，如果让我们用一句话来总结信息安全领域对管理的重要性的认识，那就是从抓好“信息安全管理”（如 BS 7799-1）到建立“信息安全管理体系”（如 ISO 27001），是人们在信息安全认识论上一个质的飞跃。

视野与角度。截止目前，我们和本书的读者一起讨论的内容主要是站在一个第三方测评机构——“如何去测评别人”的角度来展开的。与作为第三方机构进行信息安全等级测评和风险评估（特别是委托式风险评估）不同，ISMS 着重建立的是组织自身的信息安全管理体系，这里所说的“组织”既包括被测评的单位，也包括测评机构本身。一个测评机构本身要建立严格的 ISMS 体系，只有这样，其服务质量才能有一个统一的评判并获得用户的认可。被测评机构建立 ISMS 的目的则是获得自身的信息安全，并有一个“长治久安”和可持续性发展的质量保障。因此，从信息安全质量管理体系这个角度来讲，ISMS 具有普适性。

那么什么是 ISMS 的核心思想呢？简单通俗地讲就是三句话：

“把你想做的事情形成文档”；

“按照文档做你想做的事”；

“你做事的每一个细节都要记录在案”。

13.2　ISMS主要内容

首先向读者介绍 ISMS 的基本要求。

ISMS 基本要求（Basic Requirements of ISMS），指组织应在其整体业务活动中，并在其所面临风险的环境下，建立、实施、运行、监视和评审 ISMS，形成文件并保持和改进其有效性文档化的 ISMS。

这是一段颇为拗口的文字。形象地讲，就是为了建立随着信息海洋的浪潮因势而变的安全大厦——信息安全管理体系，ISMS 要求一个组织严格地“照章办事”。

下面对 PDCA-ISMS“戴明环”的 4 个环节逐一进行解释。这 4 个环节代表了 ISMS 的全部内容。为了帮助读者体会 ISMS 各个环节的“烦琐要求”，我们将在 PDCA-ISMS“戴明环”的各个环节，适时利用本书前面所介绍的有关信息安全等级测评、风险评估、应急响应等方面的案例进行解释。读者应当在今后的工作中逐步认识 ISMS 与信息安全等级保护、信息安全风险评估等之间的相互关系，因为这是中国信息安全领域中正在梳理的一个核心框架问题。



自从 20 世纪 80 年代末中国开始推广 ISO 9000 等质量体系认证以来，众多企业争先恐后地纷纷通过了这些国际认证。然而直至今日，仍然有不少通过了 ISO 9000 等质量体系认证的企业频频出现重大的产品质量问题（如刚刚发生的“三鹿奶粉”事件）。我们到底是将 ISO 认证当作一个奖状挂在门上呢？还是真正按照质量体系的要求去照章办事呢？

13.2.1　计划（Plan）

计划是指规定你应该做什么并形成文件。建立与管理风险和改进信息安全有关的 ISMS 方针、目标、过程和程序，以提供与组织整体方针和目标相一致的结果。

组织对其所追求的信息安全方针、目标等安全战略层面的思考，要与组织的业务战略这个最高层面的战略方针及目标相匹配。这就是我们在本书中处处强调的“安全服务于业务”的思想。

ISMS 计划环节的首要任务是建立 ISMS 体系，包括它的范围、方针、风险评估和管理、管理者授权实施和运行 ISMS、适用性声明等。初次接触 ISMS 的读者可能对有些概念，如“管理者授权实施”、“适用性声明”等不太熟悉，这些将在后面逐一解释。

1．范围

建立 ISMS 框架，首先要明确 ISMS 框了哪些对象在其中，即 ISMS 的范围：根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 的范围和边界，包括对范围的任何删减的详细说明和正当性理由。

所谓范围，就是确定本组织 ISMS 的边界应该划在哪里。如果将一个组织的业务范围想象成一个大圆圈，那么 ISMS 的范围就是其中的一个（同心）小圆。显然，一个组织的信息化程度越高，它的业务对信息系统的依赖性就越强，信息化对业务的覆盖范围

就越紧密，这两个同心圆就逐渐趋于一致，反之亦然。因此，在确定 ISMS 的管理范围的时候，计划的制定者一定要清楚本组织信息系统对组织整体业务的“覆盖率”。

2．方针

ISMS 管理范围的“圆圈”勾画出来之后，就需要确定这个圆圈的圆心在什么地方：根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 的方针。ISMS 的方针应反映以下内容：

（1）设定 IMSM 目标的框架和建立信息安全工作的总方向和原则。例如，在“资产识别”这章中举的“数字兰曦”案例，其信息化建设的总体方针是：“推进管理量化能力，实现快速响应能力，提升科学决策能力，增强整体竞争实力”（见第 7 章“资产识别”）。兰曦公司信息安全工作的总方向和原则就应该与这个信息化方针“遥相呼应”。

（2）考虑业务和法律、法规的要求，以及合同中的安全义务。例如，中国《计算机信息系统安全保护条例》等法律和法规要求信息系统必须实施等级保护制度，通信营运服务商或信息安全服务机构要与用户签署的服务协议（SLA）和安全保密协议等。

（3）在组织的战略性风险管理的环境下，建立和保持 ISMS。这里所谓的战略性风险，不是指信息安全风险，而是指组织所处的大环境面临的风险。例如，企业面临的各种竞争环境，政府部门需要应对的各种潜在的不稳定因素等。换言之，就是组织的业务战略所面临的“大风险”。针对这个更宽泛的风险，组织应有一套风险管理措施。ISMS 则是为这个更大的风险管理服务的。

（4）建立风险评价的准则。我们在第 10 章“风险分析”中介绍了信息安全风险赋值和风险等级等这些知识。组织则要将其纳入 ISMS 方针之中，或者说，一个组织承受信息安全风险的底线是什么。

组织的 ISMS 方针制定完成之后，必须获得 ISMS 管理者的签字批准。这既是 ISMS 文件化风格中赋予管理者的权利，更是管理者对实施 ISMS 的庄严承诺之一。

3．风险评估和管理

ISMS 与风险评估/管理的关系非常密切，或者说 ISMS 包含了风险评估和管理。由于国内外对风险评估的标准已经非常系统和规范，所以 ISMS 对于如何实施风险评估/管理没有花费过多的笔墨，而是**默认**风险评估体系是 ISMS 整体框架的有机组成部分。因此，读者在阅读本章的时候应当自觉、自信地将本书前面所介绍的有关风险评估的内容作为 ISMS 体系的核心知识。

ISMS 在计划阶段，要求文档化地确立组织的风险评估方法，即要将开展“风险评估”和“接受风险”包含在 ISMS 文件中。

（1）要在 ISMS 计划环节中明确将本组织的信息安全管理纳入风险评估。尽管国内外学术界研究了诸多风险评估和管理方法，但对中国而言，依照国家有关信息安全等级保护和风险评估的系列标准开展信息系统安全等级保护和风险评估/管理，就是最基本的方法。

（2）制定接受风险的准则，识别可接受的风险级别。这部分内容我们在本书有关风险评估的章节中已经进行了充分的介绍。因此，ISMS 计划的制定者只需将其凝练出来的准则、可承受的最低风险级别等写入计划之中即可。

ISMS 要求**可比较**和**可重现**所选择的风险评估方法产生的结果。因此，组织的信息安全风险评估应该是一个长期、定期、可持续的工作。每一次评估所获得的结果最终汇集起来就形成了这个组织信息安全风险评估的历史记录，也常常称为**基准**（benchmark）。这个基准既从历史发展的脉络反映了组织信息安全管理水平是否与时俱进，也反映了与同行业相比该组织处于什么样的位置。必要的时候（如需要进行复核复检的时候），按照同样的风险评估过程得到同样的结果。

ISMS 计划中对识别、分析和应对风险的要求概况为以下 10 个方面。

（1）识别 ISMS 范围内的资产和责任人（见本书第 7 章）；

（2）识别资产所面临的威胁（见本书第 8 章）；

（3）识别可能被威胁所利用的资产脆弱性（见本书第 9 章）；

（4）识别丧失保密性、完整性和可用性之后可能对资产造成的影响（如在第 11 章“应急响应”中介绍的业务影响分析 BIA）；

（5）根据主要的威胁和脆弱性、对资产的影响及当前所实施的控制措施，评估安全失效发生的现实可能性（即安全事件发生的概率，见本书第 10 章中有关“风险计算”相关内容）；

（6）估计风险的级别（见本书第 10 章）；

（7）确定风险是否可以接受，或者是否需要按照组织所确立的风险接受准则来处理（见本书第 10 章）；

（8）采取适当的控制措施以降低或规避风险（见本书第 10 章）；

（9）在明显满足组织的方针策略和接受风险准则的条件下，有意识和客观地接受风险（见本书第 10 章）；

（10）最后，组织的管理者应对本组织面临的残余风险有所了解并批准 ISMS 计划中提出的残余风险控制方法。

上面的内容相信读者已经非常熟悉，所以不再赘述。ISMS 的制定者只需根据风险评估中的相关知识凝练出 ISMS 计划中需要的条款即可。

4．管理者授权实施和运行ISMS

获得管理者对实施和运行 ISMS 的授权是 ISMS 对管理者的要求，并且应该明确地写入计划之中。在由组织的管理者授权实施和运行 ISMS 的时候，首先要有一个“适用性声明”。我们在前面介绍过，ISMS 具有普适性，任何一个单位都可以建立自己的 ISMS。但一个组织的 ISMS 应该有其自身的特点，或者说应该根据普适性原则来“量体裁衣”。因此，ISMS 计划制定环节的最后要特别强调本单位 ISMS 计划的适用性。

5．适用性声明

适用性声明（SoA，Statement of Applicability）应从以下 3 方面进行准备。

（1）包括上面所描述的选择控制目标和控制措施，以及选择的理由。例如，本组织所划定的 ISMS 管理范围、方针，所选择的风险评估和管理措施的理由等。换言之，适用性声明就是整个 ISMS 计划的摘要。

（2）包括当前实施的控制目标和控制措施。例如，根据本单位现阶段信息化建设的实际情况，ISMS 应该重点保护的安全目标和所采用的安全措施等（见本书第 10 章“风险分析”中有关安全解决方案内容）。

（3）对任何控制目标和控制措施的删减，以及删减的合理性说明。例如，现阶段本单位重点是“系统加固”，下一阶段是“系统改造”（见本书第 10 章“风险分析”安全解决方案有关内容），这样做的理由是什么等。

这个适用性声明将作为本单位 ISMS 文档计划的最后部分，由管理者或其授权人签字申明生效。

这里反复向读者强调，ISMS 是一个文档化的并且要求严格、照章办事的管理体系。从本书在信息安全测评和风险评估等有关内容介绍过程中，读者可以看到我们对要求规范化文档的“一片苦心”，因为这是一个训练有素的安全工程师必备的素质，也是一砖一瓦打造中国信息安全保障体系的必然需要的发展趋势。理解了这一点，读者对下面 ISMS 的文件要求就不会过于反感了。

6．ISMS文件要求——文件的作用

ISMS 文件的作用包括如下 6 个方面：

（1）是指导组织有关信息安全工作方面的内部“法规”——使工作有章可循、有序开展。

（2）是组织实际工作的标准。ISMS 文件是根据 ISMS 标准和组织需要“量身定做”的实际工作的标准。对一般员工来说，在其实际工作中，可以不过问 ISMS 标准（如 ISO/IEC 27001:2005 或中国的相关标准），但必须按照消化吸收后制定的本单位的 ISMS 文件要求执行。

（3）是安全控制措施（如安全解决方案等）的重要部分。例如，我们在前面介绍了关于如何开展等级保护测评和风险评估工作。这些工作的目的是发现安全隐患、解决安全问题。为此，被测单位就会根据发现的各种安全问题进行整改，也就是要制定安全解决方案。这些安全解决方案本身就应当是本单位 ISMS 文件的组成部分。

（4）提供客观证据，即为满足相关方要求（如组织定期接受上级主管部门的安全检查），以及为持续改进组织本身信息安全管理质量提供依据。还是以上面提到的等级保护测评、风险评估和相应的安全解决方案为例，在根据各种测评结论和安全解决方案进行系统的整改之后，可以提供相关的证据（如再次进行测评）来说明本组织信息安全工作得到了不断地改进。

（5）提供组织内部安全培训的依据。例如，进行整改之后，对各种新的安全管理的规章制度、新的安全设备或技术和应急响应计划等均需要进行内部培训。而这些“文件化”的新规章制度、设备说明书、技术报告和改进后的应急响应计划等均为内部培训的内容考核等提供了丰富的素材。

（6）提供 ISMS 审核（包括内审和外审）的依据，这个审核包括 ISMS 文件审核、ISMS 认证机构专家组的现场审核等。例如，信息系统安全等级需要定期进行审核，组织在申请通过 ISMS 认证的时候需要 ISMS 认证机构的现场审核，一个通过了 ISMS 认证的组织也需要进行定期审核。专家们在进行审核的时候，最主要的工作就是根据国家有关标准逐一对组织的 ISMS 文件进行核对，从中寻找需要进一步改进的地方。

无论一个组织是准备申请通过 ISMS 认证，还是在工作中具体实施 ISMS（这一点应该是更为重要的），都必须形成、保持和不断完善一个文档体系。下面就是 ISMS 必备的文档体系。

7．ISMS必备的文档

ISMS 必备的文档包括如下 11 项内容。

（1）文件化的 ISMS 的方针、目标和范围。

（2）风险评估方法的描述。

（3）风险评估报告。

（4）风险处理计划（如安全解决方案）。

（5）文档控制程序文件。控制程序是一个组织在信息安全工作中“程序正确性”的具体体现，是控制文件质量的必要保障，这个控制程序（或流程）本身也是 ISMS 文档的组成部分。它主要包括对以下控制程序的描述：

① 文档发布前要获得主管部门负责人的批准，以确保文档的“合法性”。

② 必要时对文档进行再评审、更新和再批准，如对 ISMS 的各种文档要求每年至少评审一次。

③ 确保文档的更改和现行修订状态得到标识，如文档的更改日期、现在处于“发放”或是“作废”状态等都属于标识的手段。例如，可采用国家有关档案管理和分类的标准或组织内部档案管理方法，对 ISMS 文档版本进行标识，从而使得使用者对 ISMS 各种文档的可用性一目了然。

④ 确保在适用处获得适用文档的相关版本，如可借鉴本书第 11 章“应急响应计划”的管理模式来理解这一要求。

⑤ 确保文档对需要的人员可用，并依照文档识别的类别规程进行传输、存储和最终销毁。由于 ISMS 文档中将涉及大量组织业务中敏感性内容，甚至涉及国家秘密的内容，因此要在文档控制程序中予以明确描述，确保文档的分发得到控制。

⑥ 确保外来文档得以识别，外来文档与组织自身的 ISMS 文档应当一体化管理。所谓外来文档，既可能是组织的上级主管部门下发的有关信息安全工作的文件，也可以包

括国家制定的有关法律、法规、政策和标准等。因此外来文档应该与组织自己制定的 ISMS 文档在标识上有所区别。

⑦ 防止继续使用作废文档。在某些情况下，组织以往制定的 ISMS 文档可能会作为历史资料予以保存。因此，应当将这些已经过期了的文档明确地标识出来（如盖上“作废”的章）。

（6）有记录控制程序文件。严格地讲，“记录”本身不是“文件”，但是它属于 ISMS 文档。所谓“记录”，是将人们在执行 ISMS 工作的活动真实地记载下来。因此随着时间的推移，在 ISMS 文档体系中各种记录文档所占的比例是最大的。记录是我们评审 ISMS 是否在这个组织内部得以严格遵照执行时的最主要“物证”。因此，一个组织在 ISMS 计划阶段，就要打好记录控制程序的基础，并将如何做好记录的方法形成文件。“记录控制程序”文档要阐述以下 4 方面内容：

① 建立了哪些记录及记录是如何保持的？这些“记录文档集”应随着 ISMS 有关活动而不断增加。

② 对记录保管、保护和控制的措施是什么？记录的标识、存储、保护、检索、保存期限和处置所需的控制措施应形成文件并实施。记录还应保证清晰、易于识别和检索。这可参照上面所介绍的文件管理方法。

③ 记录控制程序中要特别注意描述如何保留过程执行记录，以及所发生的与 ISMS 有关的重大安全事件的记录。例如，重大信息安全事件报告单等。

④ 记录应考虑相关法律、法规要求和合同义务。

（7）有内部审核程序文件。ISMS 是否真正得以严格执行，组织的内部审核必不可少。因此，在 ISMS 文档体系中要包括如何进行内部审核的程序性文档，其目的是按照 ISMS 规定的时间间隔进行 ISMS 执行情况的内部审核，以确认 ISMS 的控制目标、控制措施、过程与规程的一致性。该程序性文档主要用于规范下列 5 种审核程序：

① 是否符合 ISMS 及其相关法律和法规的要求。

② 是否符合已确立的信息安全要求。

③ 是否得到有效的实施和连续贯彻、执行。

④ 是否按预期规定执行。

⑤ 如何确认所有的审核计划、记录和报告均按照有关文档的规定形成了文档。

（8）纠正措施程序文件。纠正措施是指在审核（内部审核或外部审核）ISMS 执行情况过程中所发现的问题是否得到改进。读者可以用前面介绍的等级保护测评和风险评估等方面的知识进行类比理解，如用户对在测评之后发现的安全隐患是否进行改进，改进的措施是否有效等。ISMS 从制度上对一个组织是否制定了纠正措施程序提出了明确要求。纠正措施程序文件内容应包括：

① 应识别不符合项。例如，管理者没有按照 ISMS 的相关规定进行每年度的 ISMS 评审。这就是一个不符合项。不符合项是在进行 ISMS 等质量体系评审中常用的一个术

语。评审专家经常按照国际和国内的有关标准（如 ISO 27001–2005），采用列表检查（check list）的方式来发现不符合项。

② 要确定存在不符合项的原因。例如，组织没有进行安全意识培训的原因是什么？是因为没有执行相关规定，还是培训内容已经不符合现状要求？或者没有适合的培训教师？没有培训经费等。

③ 评价杜绝不符合项发生的措施需求。为了保证杜绝不符合项发生，需要采取什么措施和需要什么资源等。

④ 记录所采取纠正措施的结果。例如，对系统进行了安全加固之后，实事求是地记录加固是否有效。

⑤ 评审所采取的措施。根据记录等进行评审，评价纠正问题的措施是否有效。

（9）预防措施程序文件。在介绍风险评估和应急响应等相关内容的时候，都提到未雨绸缪，因为预防比事后处置更有效。ISMS 也对保证预防措施程序的正确性提出了相应要求。预防措施程序文件应包括：

① 识别潜在的不符合项及其原因。

② 评价防止不符合项发生的需求措施。

③ 确定和实施所需要的预防措施。

④ 记录所采取措施后的结果。

⑤ 评审所采取的预防措施。

（10）适用性声明文件。

（11）ISMS 的管理评审程序文件。管理评审体现了一个组织的决策层对 ISMS 是否真正重视。ISMS 要求对如何实施管理评审有一套规范化的流程。管理评审程序文件包括如下内容：

① 组织的管理者应按照计划规定的时间间隔（至少每年一次）评审 ISMS。

② 评审 ISMS 的符合性，即按照国家有关 ISMS 的标准来评审该组织的 ISMS 建设在多大程度上符合国家标准的要求。

③ 评审过程应记录在案，评审结论应形成文件。

8．ISMS对管理者职责的要求

信息安全是一个组织业务战略的重要组成部分，组织要赋予负责 ISMS 的管理者相应的职权来履行职责。例如，一个公司的董事会应该赋予 CEO 相应的管理职责，CEO 又应该在这个职责范围内授权给 CIO（首席信息技术主管）或 CISO（首席信息安全技术主管）以相应的 ISMS 管理权限。这些要求包括以下 3 个方面。

（1）管理承诺。所谓管理承诺，就是管理者要以书面保证的形式来承诺履行 ISMS 赋予管理者的职责，它包括如下内容。

① 制定 ISMS 方针。

② 确保 ISMS 的目标和计划得以制定。

③ 落实信息安全的角色和职责。例如，组织的信息安全、应急响应的负责部门、管理和技术队伍的组成，对安全员、审计员和系统管理员的任命等。

④ 向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性。例如，组织定期进行信息安全知识的培训和应急演练等。

⑤ 提供足够资源，以建立、实施、运行、监控、评审、保持和改进 ISMS。

⑥ 决定接受风险的准则和可接受风险的级别。本组织承受风险的原则、最低限度等，必须由管理者来决定。

⑦ 确保 ISMS 内部审核的执行。

⑧ 实施 ISMS 的管理评审。

（2）资源管理。组织应赋予管理者相应的权利，并提供相应的资源，以确定并提供信息安全工作所需的资源——人、财、物。

（3）培训、意识和能力。组织应确保所有分配有 ISMS 职责的人员具有执行所要求任务的能力；确保所有相关人员意识到其信息安全活动的适当性和重要性，以及如何为实现 ISMS 目标做出贡献。

至此，我们完成了建立 ISMS 文档化计划的主要工作。读者可以将这一庞大的文档计划制定工作理解为组织 ISMS 大厦的设计蓝图。在蓝图确定之后，ISMS 的第二步就是实施了。

13.2.2　实施（Do）

简单说，实施即做文件规定的事情。严格遵照计划阶段制定的 ISMS 文档，实施和运行 ISMS 方针、控制措施、过程和程序。实施 ISMS 的主要工作包括以下 7 方面。

（1）制定风险控制计划。例如，制定风险评估计划及风险评估工作结束后要制定安全解决方案等。

（2）实施风险控制计划。例如，进行风险评估，根据安全解决方案进行系统加固、改造和升级等。

（3）度量所选择的控制措施的有效性。例如，整改完成之后进行剩余风险的评估，评价其是否满足承受风险的最低限度。

（4）实施培训和意识教育计划。例如，按照培训计划进行安全意识、安全技能、应急演练等培训。要注意整个过程需要记录在案并评估其有效性。

（5）实施安全事件响应计划。根据 ISMS 制定的计划（其中就包括如应急响应计划等），对突发安全事件进行处置。同样要注意整个处置过程的记录和事后评估。

（6）管理 ISMS 的运行。例如，按照计划阶段确定的要求，组织 ISMS 的定期评审，以及评审后的改进等。

（7）管理 ISMS 的资源。管理者应当通过对 ISMS 资源的优化管理，来体现一个组织决定进行 ISMS 建设的正确性和有效性。事实上，有一些 ISMS 不成功的案例并非组

织机构没有决心或者没有投入，而是对投入的成本效益没有进行科学的分析和有力的展示。

为了全方位地关注一个组织整体信息安全质量体系的建设情况，ISMS 的第三个环节就是对实施情况进行检查。

13.2.3　检查（Check）

检查即评审所做事情的符合性。对照 ISMS 方针、目标和实践经验，评估 ISMS 执行过程的具体情况，并将结果报告管理者以供评审。评估内容包括以下 4 方面。

（1）ISMS 的执行程序及其他控制措施是否得以认真贯彻。

（2）是否对 ISMS 的有效性定期评审。

（3）度量控制措施的有效性以验证安全要求是否被满足。

（4）是否按照计划的时间间隔进行风险评估的评审等。

有的读者可能觉得上述评估要求的描述不太容易理解。建议有这种感觉的读者可以借鉴本书前面介绍的信息安全等级测评检查、风险评估等内容来理解。但是，需要向读者说明的是，ISMS 的检查虽然包括这些“事务性”的内容，但却更关注如何通过这些事务性的测评检查来发现组织在实施 ISMS 过程中有哪些不足之处。

在对一个组织的 ISMS 执行情况进行评估的时候，ISMS 规定了要具备的输入条件和输出结果。

输入条件包括：

（1）ISMS 审核和评审的结果。例如，ISMS 年度评审的各种文档等。

（2）相关方的反馈。例如，在对一个信息安全风险评估机构进行 ISMS 检查的时候，相关方的反馈就包括被测评机构的服务问卷调查表等。一个软件企业在进行 ISMS 评估的时候，相关方的反馈就包括用户对该企业生产的软件的评价、Bug 修改的情况等。

（3）组织用于改进 ISMS 执行情况和有效的技术、产品或程序。例如，新设立的信息安全岗位、人力资源配置和新增的安全投入预算等。

（4）预防和纠正措施的状况。例如，风险评估报告、安全解决方案实施后的测评报告等。

（5）以往风险评估没有充分强调的脆弱点或威胁。例如，随着信息系统或者业务战略发生改变所出现的新的安全风险评估报告等。

（6）有效性度量的结果。例如，风险分析报告（含风险等级等相关数据）等。

（7）以往管理评审的跟踪措施。例如，以前组织没有建立专门的信息安全机构，现在是否得以改进及怎样改进等。

（8）可能影响 ISMS 的任何变更情况。例如，主要的 ISMS 管理者离任后，继任者的履历情况介绍等。

（9）改进的建议。例如，第三方测评机构出具的信息安全整改要求等。

输出结果包括 ISMS 有效性的改进评估报告。这是 ISMS 检查环节完成之后输出的一个总体评估报告。它包括风险的改进，是否需要修改一些陈旧的安全事件响应流程，是否需要新增资源等。如果有必要，可以将其中一些细节性技术报告（如风险评估和风险处理计划的更新等）作为总报告的支撑附件。

ISMS 的第四个环节是在检查所发现的问题或不足的基础上，进行纠正或预防。

13.2.4　处置（Act）

处置指采取纠正和预防措施，持续改进 ISMS。基于 ISMS 的检查结果或者其他相关信息，采取纠正和预防措施，以不断改进，保证 ISMS 的有效性。

在这一阶段，一个组织应经常：

（1）实施已发现的 ISMS 需要改进的措施。例如，对在风险评估中发现的脆弱性应该尽快加以改进等。

（2）从其他组织和组织自身的安全经验中吸取教训。

（3）与所有相关方沟通执行措施和改进措施情况。例如，一个组织在进行了等级保护测评、风险评估、应急响应演练之后所发现的问题，应该向上级主管部门或安全服务机构、设备集成提供商等进行汇报、沟通和磋商。

（4）确保改进达到了预期目标。

最后值得提及的是，2006 年，中国国务院信息化领导小组办公室等信息安全主管部门在北京、上海、深圳等信息化发达城市进行了 ISMS 试点，参与单位既包括政府部门，也包括传统的钢铁企业，涉及民生领域的医疗保障单位和事关国家金融安全的证券交易机构等，并取得了一批丰硕的成果，初步验证了 ISO 27001−2005 等相关国际标准在中国的适应性，为最终确立中国自己的国家标准打下了坚实的基础。

然而，中国在推广实施 ISMS 的过程中仍然存在一些尚待解决的问题。

（1）ISMS 在法律和法规层面的定位问题。读者可能已经注意到，在实施 ISMS 的过程中，我们经常要求按照国家相关法律和法规来实施 ISMS。所以，如何在信息安全立法的战略层面纳入 ISMS 的相关要求，是今后工作中应当关注的问题。

（2）ISMS 框架与其他信息安全标



能力成熟度模型（CMM）是美国卡内基梅隆大学软件工程研究所（www.sei.cmu.edu）于 1991 年提出的软件质量管理体系，并在国际 IT 界获得了成功的运用。1993 年 4 月，美国国防部所属的国家安全局（NSA）“民技军用”，将 CMM 的概念引入到了系统安全工程（SSE）之中，从而衍生出了 SSE-CMM 工程标准。该标准也是目前国际上对信息系统进行等级保护时经常采用的手段之一。由于中国尚未出台相关的国家标准，故作者并未将有关 SSE-CMM 的介绍纳入本书之中。但中国已经有某些重要的测评机构在测评工作中参照了该工程标准。

准的衔接。从国内、外信息安全实践的情况和整体性地应对安全威胁的发展趋势来看，ISMS 应该是一个能够将信息安全等级保护、风险评估、信息安全系统保护能力评估（SSE-CMM）、应急响应、容灾备份等相关标准规范有机地融合在一起的体系框架。但在这些既有密切关联、又各有其侧重点的标准体系之间，哪些是共同的控制措施？如何对它们进行有效的裁剪？一个组织既要根据等级保护来建设自己的信息系统又要对系统进行风险评估，还要建立 ISMS……如何使一个组织投放的安全资源获得最优化的产出？等等，这些问题都有待于解决。

（3）ISMS 本身的适用性问题。尽管 ISMS 代表了国际信息安全领域对驾驭安全风险的先进思潮，但如果一味生搬硬套 ISMS 的教条，不根据自身的特点来改造甚至创新 ISMS 的运用，那么 ISMS 的效果就会大打折扣，甚至成为费力不讨好的苦差。

最后，作为全书的结束，总结一下本书所涉及的信息安全等级保护、风险评估和信息安全管理体系这三大标准体系之间的关系。

中国的法律和法规要求信息系统必须进行等级保护。这是中国开展信息安全保障工作的基本制度。

风险评估和 ISMS 均是为了实现等级保护而开展的具体工作，或者说为了实现等级保护而采取的技术路线。

风险评估是 ISMS 的核心组成部分。

13.3　本章小结

- ISMS 产生的历史
- 从信息安全管理到信息安全管理体系
- 制定 ISMS 的国际标准化组织
- 戴明环与 ISMS
- ISMS 的适用对象
- ISMS 的总体要求
- 建立 ISMS 的环节
- 计划 ISMS 阶段需要注意的问题
- 实施 ISMS 阶段需要注意的问题
- 检查 ISMS 阶段需要注意的问题
- 处置 ISMS 阶段需要注意的问题

尾声：实力源于何处

一个国家，除了“硬实力”，还有越来越重要的“软实力”。

什么是“硬实力”？“硬实力”就是一个国家所具有的经济实力和军事实力。

什么是“软实力”？“软实力”比“硬实力”复杂一点。“软实力”主要是文化、价值观、意识形态和民意等方面的影响力。

“软实力”（Soft Power）的概念是由美国哈佛大学教授约瑟夫·奈提出来的。根据约瑟夫·奈的说法，硬实力是一国利用其军事力量和经济实力强迫或收买其他国家的能力，软实力则是“一国通过吸引和说服别国服从你的目标从而使你得到自己想要的东西的能力”。约瑟夫·奈教授认为，一个国家的软实力主要存在于三种资源中：“文化（在能对他国产生吸引力的方面起作用）、政治价值观（当这个国家在国内、外努力实践这些价值观时）及外交政策（当政策需被认为合法且具有道德威信时）。”另外，美国学者尼古拉斯·欧维纳则认为：“军事以外的影响力都是软实力，包括意识形态和政治价值的吸引力和文化感召力等。”

如果说“信息安全技术”是一种“硬实力”，那么“信息安全管理”就是一种“软实力”，没有后者，“硬实力”往往难以有效发挥，昂贵的设备可能变得形同虚设。

在某种意义下，“软实力”比“硬实力”更重要。在信息安全中，常强调“三分技术七分管理”就是这个道理。正如一个强国，不仅要靠强大的武装，还要靠精神的辐射；正如一个强人，多半不是靠伟岸的身躯，而是靠伟大的灵魂。

观感

（1）在中国，ISMS 与信息安全等级保护和风险评估的相互关系是什么？您认为这三者之间是一个什么样的关系？

（2）根据本书前半部分有关巴山市电子政务信息系统——“天网”的介绍，请您给出巴山市政府信息中心建设 ISMS 要注意的问题。

（3）根据本书后半部分有关兰曦公司的介绍，请您给出兰曦公司建设 ISMS 要注意的问题。

（4）根据本书“应急响应”的介绍，请您给出“南海大学”网络信息中心建设 ISMS 要注意的问题。

（5）根据本书虚拟信息安全测评机构——“深海”信息安全测评中心所从事的信息安全等级保护测评和风险评估工作，请您给出“深海”信息安全测评中心建设 ISMS 要注意的问题。

（6）如果您是一家大型 IT 企业的 CEO，请您制定一个该企业通过 ISMS 认证的计划。

参 考 文 献

[1] 许国志，等．系统科学．上海：上海科技教育出版社，2000．

[2] 许国志，等．系统科学与工程研究．上海：上海科技教育出版社，2000．

[3] 王文华．钱学森实录．四川：四川文艺出版社，2001．

[4] 王元，华罗庚．南昌：江西教育出版社，1999．

[5] 钟义信．信息科学原理．北京：北京邮电大学出版社，2002．

[6] 关义章，等．信息系统安全工程学．北京：电子工业出版社，2002．

[7] （美）阿奎拉，等．决战信息时代．宋正华，等译．长春：吉林人民出版社，2001．

[8] Stallings W．CRYPTOGRAPHY AND NETWORK SECURITY, Principles and Practice．Prentice Hall, 1999．

[9] Jain.R．THE ART OF COMPUTER SYSTEMS PERFORMANCE ANALYSIS, Techniques for Experimental Design, Measurement, Simulation, and Modeling.Wiley, 1991．

[10] Bishop M．Computer Security：Art and Science．冯登国，编译．北京：清华大学出版社，2004．

[11] （美）赖尔，等．启蒙运动百科全书．刘北成，等编译．上海：上海人民出版社，2004．

[12] （美）维纳．控制论：或关于在动物和机器中控制和通信的科学．郝季仁，译．北京：北京大学出版社，2007．

[13] 姜继为．航天奇才——冯•布劳恩．北京：北京图书馆出版社，1997．

[14] （美）费米．原子在我家中．何光兆武，等译．上海：上海人民出版社，2005．

[15] 王金华，等．载人航天史话．北京：国防工业出版社，1997．

[16] 公通字[2007]43 号：信息安全等级保护管理办法．公安部，国家保密局，国家密码管理局，国务院信息化工作办公室文件．

[17] GB 17859—1999 计算机信息系统安全保护等级划分准则．

[18] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求．

[19] 信息安全技术 信息系统安全等级保护基本要求（报批稿）．

[20] 信息安全技术 信息系统安全等级保护实施指南（报批稿）．

[21] 信息安全技术 信息系统安全保护等级定级指南（报批稿）．

[22] 国信办[2005]25 号：电子政务信息安全等级保护实施指南（试行）．

[23] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求．

[24] GB/T 21028—2007 信息安全技术 服务器安全技术要求．

[25] GB/T 20272—2006 信息安全技术 操作系统安全技术要求．

[26] GB/T 20008—2005 信息安全技术 操作系统安全评估准则．

[27] GB/T 20009—2005 信息安全技术 数据库管理系统安全评估准则．

[28] GB/T 20011—2005 信息安全技术 路由器安全评估准则．

[29] GB/T 20281—2006 信息安全技术 防火墙技术要求和测试评价方法.

[30] GB/T 20275—2006 信息安全技术 入侵检测系统技术要求和测试评价方法.

[31] GB/T 18018—2007 信息安全技术 路由器安全技术要求.

[32] GB/T 20945—2007 信息安全技术 信息系统安全审计产品技术要求和评价方法.

[33] GB/T 21050—2007 信息安全技术 网络交换机安全技术要求.

[34] （德）贝克．风险社会．何博闻，译．南京：译林出版社，2006.

[35] Alberts C, Dorofee A.Managing Information Security Risks: The OCTAVE Approach．Addison-Wesley，2003.

[36] 周效坤，等．信息反恐论．北京：军事科学出版社，2004.

[37] （美）Whiman M.E.等著．信息安全管理．向宏，等译．重庆：重庆大学出版社，2005.

[38] GB/T 19716—2005 信息技术 信息安全管理实用规则.

[39] GB/T 20269—2006 信息安全技术 信息系统安全管理要求.

[40] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求.

[41] GB/T 20984—2007 信息安全技术 信息安全风险评估规范.

[42] GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理指南.

[43] GB/Z 20985—2007 信息安全技术 信息安全事件分类分级指南.

[44] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南.

[45] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范.

[46] ISO/IEC 27001-2005 Information technology—Security techniques—Information security management systems—Requirements.

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888

传　　真：（010）88254397

E-mail：　dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

　　电子工业出版社总编办公室

邮　　编：100036